~~TOP SECRET~~

ARMED FORCES SECURITY AGENCY

JF-196

49/50/TOPSEC/AFSA-14

Copy No. 34

From: AFSA-14

To: _____

Approved for Release by NSA on 3-12-2018 pursuant to E.O. 13526, MDR Case # 102061

Declassified by NSA/CSS

Deputy Associate Director for Policy and Records

On 20150121 by SG

~~TOP SECRET~~

DF 196 49/50/TOPSEC/AFSA-14

REPORT ON RUSSIAN DECRYPTION IN THE FORMER GERMAN ARMY

1. The attached is an AFSA translation of two papers submitted in July 1945 to United States authorities in Europe by German nationals, Alex DETTMANN and Sergius SAMSONOW. The longer of the two papers is entitled: "Report on Russian Decryption in the Former German Army". To it is appended a "Suggestion for Formation of a Russian Cryptanalytic Unit". Both reports were forwarded to GCHQ, London where they received the collective TICOM number 805.

2. Both DETTMANN and SAMSONOW were interrogated extensively by TICOM, and DETTMANN is particularly known for his long treatise entitled "Methods of Decipherment" which was written during a period of two years at the European Command Intelligence Center, APO 757 and which was forwarded in installments to Army Security Agency where it was issued as received. See DF-136, 138, 139, 141, 144, 145, 146, 154, 155, 156, 165, 166, 167, 168, 171, 175, 179, 180, 181. Other cryptologic studies of DETTMANN during this period were issued as DF-112, 132, and 133. DF-185 Parts I-III is a translation of the personality list prepared by DETTMANN of former members of German signal intelligence.

3. Although TICOM 805 was translated upon its receipt by Army Security Agency in August 1945, and although an English translation by the authors has been circulated under the title "Report of Russian Deciphering in the Former German Army", it is believed that only a few readers have had access to the document and that the translation does not do full justice to the inherent value of the document. With this in mind a new translation has been made and formally issued.

Translated: RWP 35 copies

May 1950 74 pages

Distribution: Normal

DF 196

TABLE OF CONTENTS

	Page
Preface	4
Report on Russian Decryption in the Former German Army	6
Introduction	9
Part I. Successes of Russian Decryption	11
Part II. Technical	26
Part III. The Structure of the Russian Cryptanalytic Section in the Former German Army and a Criticism of its Organizational Defects	54
Suggestion for Formation of a Russian Cryptanalytic Unit	59
Plates	64

DF-196

PREFACE

In the attached we submit for your consideration a report on Russian decryption in the former German Army. The materials unfortunately do not give the picture we sought to present but with the limited means at our disposal we could not do all we should have wished.

The questions treated in the report, as well as the existence of such a report, would fall within the classification SECRET MILITARY MATTER ("Geheime Kommandosache"), according to the classification rules of the former German Army. For reasons you will readily comprehend we request that the material be given a similar classification and that it be treated strictly in accordance therewith.

In addition to the statements regarding the writers in the introduction, we make the following remarks:

Alex DETTMANN (Lieutenant in the Reserve), 32 years old, married, two children, scientific worker in the field of Russian cryptanalysis, family at present living in Luebeck. Born in St. Petersburg (Russia); mother Russian; father a German (Auslandsdeutscher) wholesale merchant in glass and metal lines. German citizen since birth; resided in Germany since 1918. Two military maneuvers in peace time; at the outbreak of war with Russia remained active in the same field as Inspector in War Administration (Kriegsverwaltungsinspektor); after abolition of these grades (KV-Raenge) a short period of military service as corporal (Unteroffizier) sergeant (Wachtmeister), and Chief Warrant Officer (Oberfaehnrich). Commissioned Lieutenant in the Reserve (Leutnant der Reserve). At no time member of the NSDAP or any of its subordinate organizations.

Sergius SAMSONOW, First Sergeant (Oberwachtmeister). 40 years old, married, two children, owner of an export-import business and an agency handling bills of exchange (Devisenanwaltspraxis) in Hamburg (both dormant since the beginning of the war). Born in Irkutsk (Siberia) as son of Russian

parents, father wholesale merchant and member of the board of the Russian-Asiatic Bank in prerevolutionary Russia; emigrated from Soviet Russia in 1920 and lived without citizenship of any sort (Nansen pass) in Germany. Became a German citizen in 1930 and was called for military duty in 1940. Since February 1941 active as scientific worker on cryptanalysis. At no time member of NSDAP or of its organizations.

In turning in this report we state our readiness to serve as cryptanalysts of Russian, also to serve as organizers and supervisors of a unit for analyzing Russian material in the interest of the USA. We can confidently undertake such a task because we feel sure we have the administrative and technical ability. We therefore add to this report a brief suggestion for a set-up for analyzing Russian systems. We can guarantee that such an organization will be able to turn out decrypted Russian messages in a short time.

The project predicates calling in a number of those analysts formerly associated with us in order to make the organization productive without loss of time. It is clear that the sooner such an organization is formed the less time will be lost in warming up, because thus there would be less of a gap between the stoppage of our former work and the new work, and we should forget less detail and come nearer to maintaining the necessary continuity in following changes in the Russian cryptographic systems. Otherwise this gap may become too great to bridge.

Our willingness to assume such work depends on the assumption that due recognition will be given to the value of our work, both in the matter of pay and proper living conditions.

We again request that our names be kept secret.

23 July 1945 /signed/ DETTMANN

SAMSONOV

DF-196

REPORT ON RUSSIAN DECRYPTION IN THE

FORMER GERMAN ARMY

DF-196

TABLE OF CONTENTS

	Page
INTRODUCTION	9
Part I.	
SUCCESSES OF RUSSIAN DECRYPTION	11
A. General Importance of NKVD Organs and Their Function in Peace and War. Evaluation of Decryption	11
NKVD as Political Security Organ	11
NKVD as Protective Barrier against the Outside World	12
NKVD as Organ for Economic Control	14
NKVD and RKKA	15
NKVD as Organ of Control	15
NKVD as Organ of Training	16
NKVD as Elite Troops	16
Supplemental Tasks of the NKVD in Wartime	17
B. Intelligence Results of Decryption of Army, Air Force, NKVD, Partisan, and Agent Messages.	18
Recognition of Enemy Situation	18
Recognition of Operational and Tactical Measures	20
Recognition of Supply Situation	20
Losses of Men and Materiel	21
Replenishment of Old and Formation of New Units	21
State of Health and Morale of Troops	22
Passwords and Recognition Signs	22
Situation in Rear Areas	23
Details of Traffic and Transportation Situation	23
Details on War Production	24
Partisan Activity	24
Infiltration of Reconnaissance Groups and Agents	24
Polish Resistance Movement	24
Significance of Cryptanalysis	25
Part II	
TECHNICAL	26
A. The Russian Cryptographic Service. Its Structure and Organization	26

DF-196 Page

Army and Air Force 26

The 8th Section of the General Staff of RKKA and its Subordinate Organs. 26

Basic Changes during the War up to Spring 1945 27

NKVD

Guidance and Control of NKVD Cryptographic Systems 31

Brief Survey of Intra-state Circuits 32

Partisans, Agents, and Scouts 32

B. Development of Russian Cryptographic Systems in the Light of Cryptanalysis 33

Army and Air Force Systems 33

Operational Systems 34

Signal Tables 35

Address Codes 36

Substitution Systems 36

Transposition Systems 40

Additive Systems 42

NKVD Cryptographic Systems 43

Operational Systems 43

Substitution Systems 43

Transposition Systems 45

Additive Systems 45

Partisan, Scouts, Agent Systems 47

Encipherment and Disguise of Coordinates 48

C. Explanation of Terms 51

D. Schematic Survey of the Most Important Systems Used by Russia during the War for Army, Air Force, and NKVD (decrypted)

Part III

THE STRUCTURE OF THE RUSSIAN CRYPTANALYTIC SECTION IN THE FORMER GERMAN ARMY AND A CRITICISM OF ITS ORGANIZATIONAL DEFECTS. 54

Suggestion 59

Plates 1-11 64-74

REPORT ON RUSSIAN DECRYPTION IN THE FORMER GERMAN ARMY

INTRODUCTION

The authors of this report are the former chief cryptanalyst (Russia) of the Agency called General der Nachrichten Aufklaerung which was the controlling central office for signal intelligence in the German Army, and his deputy. The former was from 1934 on, i.e. practically from the beginning of the systematic monitoring of Russian traffic by Germany, a collaborator in the field of Russian cryptanalysis. The latter was assigned to the Agency even before the war began as one especially suited for the work, and was the closest associate of and later chief assistant to the former. Hence the two are the only persons fully competent to speak on the whole field of cryptanalysis of Russian military and political cryptographic systems, and the only persons in Germany able to compose an analytical report on the possibility of analyzing all types of Russian traffic and, if necessary, of organizing and carrying out cryptanalysis.

In addition to the authors there are doubtlessly a number of competent analysts of Russian systems; for example, at the same central Agency there are those who have worked under the authors or in out-stations of the organization. In contrast to the authors, however, these were employed on limited cryptanalytic assignments and thus do not have the same comprehensive grasp of the entire field of Russian cryptanalysis.

As those in charge of the cryptanalytic organization, the authors are also in a position to give a dependable picture of the worth of the evaluation of content of decrypted material. It can be asserted that the information from decrypted messages always proved absolutely reliable and contained important information, since the opponent under observation composed them for his own use and treated them as "SECRET". Agents' reports and statements by prisoners of war which also serve the High Command as sources of information could not compete with decrypted messages since they were often intentionally or unintentionally incorrect and incomplete. If any confirmation is needed of the statement concerning the

reliability of decrypted messages, it is only necessary to point out that in countless cases these were confirmed by captured documents, agents' reports, and interrogations of prisoners of war. Accordingly they were rated and evaluated by the High Command as "reliable information" ("verlaessliche Nachrichten").

The cryptanalytic organisation conducted by the undersigned was able to deliver valuable information right up to the end of the war. Operational and tactical utilisation was precluded for a long time, however, by lack of military potential.

PART I. SUCCESSES OF RUSSIAN DECRYPTION

A. General Importance of NKVD Organs and Their Functions in Peace and War. Evaluation of Decryption

Among the first results of decryption of Russian cryptographic systems was the recognition of the importance of the NKVD (Peoples' Commissariat for Internal Affairs) in the political, military, and economic life of the Soviet Union. It soon came out that the role of this organization was far more extensive and far more important in its influence on military matters than had previously been assumed. These facts led to devoting all possible attention to the monitoring of NKVD radio traffic.

NKVD as Political Security Organ: The basic task of the NKVD is assuring the continuance of the political structure of the USSR. Hence it exercises the sharpest kind of control over the political, military, and economic life of the country. For this purpose administrative offices are set up in every city to meet the manifold demands made on them. To carry out necessary measures the NKVD has at its disposal various types of troops of its own — NKVD troops — which are assigned and employed according to need by the Central Office in Moscow (the ГУП ВОЙСК НКВД = ГЛАВНОЕ УПРАВЛЕНИЕ ВОЙСК НКВД = Central Administration of NKVD Troops). Assignments in political supervision are carried out by the "ПОЛИТ ОТДЕЛЫ НКВД " Political Section NKVD. This is achieved by the aid of an extensive network of agents which can note and combat any trend hostile to the Soviets. The actual combatting of such movements is by contingents called " ВНУТРЕННЬЕ ВОЙСКА " Troops of the Interior. The sending away of politically unreliable elements, surveillance, and control of concentration camps as well as the setting up of penal camps and penal battalions fall in the province of the " НКВДОВСКЕ ВОЙСКА НКВД Direct Troops. With the occupation of foreign territory during the war, the number of political sections increased materially because the occupied

territories, as a result of their often quite different political organization, required very intensive supervision. Consequently a very great increase in the contingent of Troops of the Interior became necessary.

NKVD as Protective Barrier against the Outside World: Corresponding to the special political structure of the USSR, it was necessary to provide for sealing the country hermetically from the outside world. This called for the formation of an effective and reliable frontier guard, which was provided by the ПОГРАНИЧНЫЕ ВОЙСКА НКВД Frontier and Security Troops. Only the easily guarded short stretches were originally left to the Army for protection. Since the beginning of 1939 even these parts have been taken over by the Frontier Troops. Corresponding to their task, these troops have aircraft available, and, along the water boundaries, appropriate watercraft. Even in 1935-1937 the organization, tasks, effectiveness, and strength of these troops could be ascertained from decrypted messages originating in several frontier guard areas.

Radio traffic could be read, for instance, from frontier and coast guard areas:

1. NORTH (Control Station Murmansk): Petschora to Gulf of Finland.
2. LENINGRAD (Control Station Leningrad): Carelian Isthmus
3. ODESSA (Control Station Odessa): Bessarabia to east coast of the Crimea.
4. NOVOROSSISK (Control Station Novorossisk): Sea of Asof and northeast coast of Black Sea.
5. TRANSCAUCASUS (Control Stations Suchum and Baku): east coast of Black Sea, Turkish and Iranian border, west coast of the Caspian Sea.
6. KASAKSTAN (Control Stations Tashkent and Alma-Ata); east coast of Caspian Sea and land frontier in Central Asia.

DF-196

Each of these first four areas had one frontier guard unit (Abteilung); the last two had two units each of frontier guards (called first ДИВИЗИОН , later ОТДЕЛЕНИЕ). Each of the units was about the size of a reenforced regiment (Regiment), and each was divided into a number of sub-divisions (Unterabteilungen, ОТРЯД) [the number varying] according to the geographic situation. Thus the coast guard unit Odessa had five sub-divisions, based at Cherson, Otschakow, Sevastopol, Yalta, and Alupka. These sub-divisions were broken into frontier and coast guard watches (Wachen) which set up posts (Posten) of varying strength to perform the actual work of closing the frontiers. Later it was ascertained that the organization in the Far Eastern areas was the same.

From current monitoring of radio traffic of the frontier guard units, it became apparent that, with the beginning of the war, the organization of the defense of frontiers facing enemy countries underwent a basic change. Aside from an extensive adjustment of the structure of the frontier troops of the NKVD to that of the RKKA РАБОЧА КРЕСТЬЯНСКАЯ КРАСНАЯ АРМИЯ (Red Worker and Peasant Army) (subdivided into regiments and battalions) there was an essential change in assignments. It was soon learned that regiments of NKVD Frontier and Security Troops were employed some 30 to 60 kilometers behind the combat units of RKKA to form an unbroken, very mobile, and deeply deployed security zone. Of approximately 200 Frontier Guard and Security regiments recognized from decrypted traffic, about one-third was spotted as first line of this security zone, another third was employed farther to the rear, while the remaining third formed the mobile reserve. Each of the NKVD regiments of the front line guarded a sector zone 60 kilometers wide. In the course of time it could be established that some three first-line NKVD regiments were needed to guard the rear area of two RKKA armies. NKVD forward staffs controlled the employment of these regiments; these staffs were located in the immediate vicinity of the forward staffs of the Army but received their orders from NKVD headquarters in Moscow. Five to eight regiments of front-line NKVD troops were assigned to a front

sector — of which, after the capitulation of Finland, there were eleven. The task of this security zone was to prevent desertion and infiltration of enemy agents by sealing hermetically the sector of the front from the rear area; by mopping up pockets, and clearing areas near the front of cut-off enemy troops and bands; by removal or resettlement of the populace for political reasons; by return of population for repair or new construction of roads, defense installations, air fields, and plants of value to the military economy; by guarding supply; and by collecting and transporting prisoners to the rear.

It may be mentioned briefly that each NKVD Frontier Guard regiment had three battalions which consisted of several field watches and a reserve field watch. Furthermore, the battalions employed for special tasks "МАН. ГРУППЫ = МАНЕВРЕННЫЕ ГРУППЫ mobile groups, "ОПЕР. ГРУППЫ "operative groups and ОЧГ (the German term for the last abbreviation has escaped the author's mind).

NKVD as Organ for Economic Control: To the successes of decryption belongs further the early establishment of the fact that the entire economy of the Soviet Union, in particular the military economy and transportation system, was under very sharp control, and thus under the influence of the NKVD. For this purpose the NKVD used its local organs, inasmuch as these currently supervise the carrying out of economic plans set up by the state's economic planning, and report regularly to their superior offices the results of this activity. The reading of these reports, made possible by decryption, gave hints concerning the capacity of many branches concerned with war economy; often showed maladjustments therein and methods employed to correct these maladjustments. These data were especially valuable during the war since they disclosed the type and extent of the difficulties with which the economic leadership of the Soviet Union had to contend. In the course of the war the function of the NKVD was extended insofar as to the controls exercised in peace time and to the right to intervene directly if trouble arose there was added the task of caring for the return to production of

[redacted] or destroyed plants. For this purpose the offices of the NKVD controlled all specialists in their areas and supplied them with work or, in case of need, sent them to other NKVD areas. These powers were extended with the occupation of large new areas.

As an essential part of the total economy of the country, the transportation system, and in particular the railroads, were under the control of the NKVD. After the outbreak of the war it became necessary to take over protection of the railroads along with their control. This included guarding transports, depots, bridges, junction points, and important as well as threatened stretches of railroad track. To meet this task specially trained troop contingents " ЖЕЛЕЗНОДОРОЖНЫЕ ВОЙСКА НКВД " or NKVD Rail Troops were formed. The organization resembled that of the Army with a division as the largest unit. During the war three divisions of the NKVD Railway Troops were identified and their employment could be followed currently. Since the main task of decryption in the former German Army was to secure military intelligence, the influence of the NKVD on economic matters could be worked out only in fragmentary fashion, but even so the enormous significance of the NKVD for Soviet economy was clearly recognizable. Undoubtedly if full monitoring of economic internal traffic and its decryption had proved possible, as assumed, this influence on the economy would prove still more extensive.

NKVD and RKKA. NKVD as Organ of Control: Especially characteristic and revealing for the power of the NKVD is the relation of this organization to the RKKA. NKVD undertook the political direction of the RKKA beginning with the General Staff and ending with the last man, in order to guarantee the absolute Bolshevik-Communist philosophy of every member of the Red Army. For this purpose the NKVD has a system of political guidance and leadership reaching from the General Staff down to the company platoons. Through the employment of so-called "Fifth Units" ("СПЕЦ. ОТДЕЛ "(special unit) or "ПОЛИТ ОТДЕЛ" (political unit) in all staffs from the General Staff down to that of the division, and from the "ПОЛИТИОН " (political

DF-19%

commissar) and " ПОЛИТРУК " (political leader) in the lower echelons down to the platoon, the NKVD actually watches, guides, and instructs every man. In addition to the above-mentioned official representatives of the NKVD there are secret agents from the ranks of the Red Army working under these, whose task is to recognize and report in their initial stages any movements hostile to the Soviets. Arrest and punishment lie in the hands of courts martial conducted by the NKVD.

NKVD as Organ of Training: Aside from political training the NKVD is charged with training the RKKA in a number of military specialties. Among other specialities, for example, the training of sharpshooter units and the conduct of training schools for dogs and carrier pigeons were in the hands of the NKVD.

The NKVD exerts an influence not to be underestimated on the point of view of the RKKA through the fact that any changes in the ranks of higher officers require the approval of the NKVD, which also controls through its agencies the selection and training of all replacements for medium and high-grade officers.

The keeping of military secrets represents a field exposed to unusual danger. Hence it is explicable that in this field the NKVD was particularly active. Security of signal transmission depends primarily upon the reliability of the personnel concerned therewith. Hence the NKVD gave particular attention to this circle. Along with the selection and supervision of technical signal personnel, there was the keenest sifting and constant testing by the NKVD of all those engaged in cryptographic work. The technical training of these persons was also the task of special organs of the NKVD. The technical part of this paper will take this up in detail.

NKVD as Elite Troops: In various phases of the war need appeared for very daring and reliable units at danger points in the line or at points of concentration. Recourse was had to NKVD troops, some of whom were formed into so-called " ОПЕРАТИВНЫЕ ВОЙСКА НКВД " NKVD Operative Troops, which were assigned to divisions of the RKKA armies. The exact number of

such elite divisions could not be determined from decryptments, but one can reckon on at least 20 such. It is worth noting that the chief employment of these divisions came in 1942 and that after the crisis passed this fell off markedly.

Supplemental Tasks of NKVD in War: Whereas at the start of the war the NKVD was able to meet the demands upon it by using the apparatus built up during peacetime, even though great expansion of personnel was required, a new organization became necessary for combatting espionage, sabotage, and the activity of enemy agents, and this new agency took over the work in this field previously done by the general organs of the NKVD. Known as " СМЕРШ " = СМЕРТЬ ШПИОНАМ "Death to Spies", it was formed from another sub-division of the NKVD which had also been formed during the war called the NKGB НАРОДНЫЙ КОММИССАРИАТ ГОСУДАРСТВЕННОЙ БЕЗОПАСНОСТИ People's Commissariat for the Security of the State, which later became a completely independent commissariat although it still worked in close collaboration with the NKVD. In the last years of the war the " СМЕРШ " through decryptments became well enough known in regard to organization and methods of work.

To the special tasks of the NKVD in war belongs also the carrying out of the mobilization and drafting of recruits for the RKKA. Moreover, the setting up of armies and units of foreign nationality and their integration into the framework of the RKKA was a matter for the NKVD, all the more since political considerations played an important role here. The activities of partisans, scouts, and agents behind the German front, which became of such great importance in the last two years of the war, were — at least in regard to training and directives — likewise the work of NKVD. To the same realm of tasks imposed by the war belong: the formation and employment of labor battalions by recruiting; workers among the people of occupied areas for work of military importance.

Mention must also be made of the fact that NKVD offices and their organs — NKVD troops of different categories — discharged their important, manifold, and often far from simple tasks in astonishingly speedy and uncompromising fashion. Of course as decrypted material showed, this was sometimes accomplished by the use of anything but humane methods.

Account is taken of the difficulty of the service required of NKVD organs by giving its units a special standing in the USSR. From decrypted messages on the subject it could be ascertained that the pay of the NKVD was essentially higher than that of the RKKA, and its subsistence appears to have been better.

The above statements, made possible by the results of years of decryption, give a sketch of the structure and importance of the NKVD apparatus. In what follows such details of cryptanalysis will be treated as may be of greatest importance to one's own conduct of war, despite the brief period during which they are significant.

B. Intelligence Results of Decryption of Army, Air Force, NKVD, Partisan, and Agent Messages

Recognition of Enemy Situation: The most important task of cryptanalysis is beyond doubt an exact, speedy, and exhaustive clarification of the enemy situation, i.e. the current determination of the location of all enemy units in and behind the front. This task was fulfilled satisfactorily during the entire course of the war by decryption, either through decryption of enemy messages dealing directly with such location or through decryption of those messages which revealed indirectly such location. Not infrequently was it possible to know of impending movements. The following examples are designed to show the type of such messages:

Dealing directly with location:

" TO THE CHIEF OF STAFF OF THE 267TH INFANTRY DIVISION. THE COMMAND POST OF THE 1032D INFANTRY REGIMENT IS IN THE WOODS 2.5 KM NORTH-EAST OF IVANOVO.

REGIMENTAL COMMANDER PETROV"

DF-196

Dealing indirectly with location:

"TO THE CHIEF OF STAFF.
ON 12.8.44 at 0750 HOURS THE RED ARMY SOLDIER KOTLOV, PETR VASSILJEVITSCH WAS PICKED UP AT THE SOUTH EXIT OF THE VILLAGE DOLGAJA BY A PATROL OF THE 15TH FIELD WATCH. THE MAN ARRESTED DESERTED THE TRENCHES BEFORE FROM THE 642ND INFANTRY REGIMENT OF THE 111TH INFANTRY DIVISION OF THE 16TH ARMY.
LEADER OF THE FIELD WATCH KOMARENKO"

Dealing with impending movements:

"THE RADIO STATION OF THE 267TH CAV. RGT. IS PACKING UP.
WE ARE MOVING TO BOLOTJE.

DIRECTOR OF RADIO STATION"

Not less important for one's own troop command is timely recognition of attack or counterattack by the enemy, since this makes possible the taking of countermeasures. The decryption section was frequently in a position not merely to deduce such intentions from various circumstantial details but also to hand on in the original words the enemy's direct orders for attack or counterattack.

Example of a direct command to attack: (System: Operations Code)

"TO COMMANDERS AND CHIEFS OF STAFF OF 172ND, 178TH, 192ND, 193RD, INFANTRY DIVISIONS, 73RD and 112TH TANK BRIGADES.
THE COMMANDER IN CHIEF OF THE ARMY HAS ORDERED:

1. 172ND INFANTRY DIVISION ATTACKS ON 14.6.43 at 0430 HOURS WITH THE 460TH INFANTRY REGIMENT IN THE DIRECTION OF GORODOK AT 1030 HOURS. WITH THE 461ST and 512TH INFANTRY REGIMENTS THE PASSAGES OVER THE RIVER KLINKA 3 and 5 KM SOUTHEAST OF GORODOK ARE TO BE FORCED AND THE ARRIVAL OF THE 112TH TANK BRIGADE IS TO BE AWAITED THERE.

2. 178TH INFANTRY DIVISION .....

3. .....
ETC. LIKE ORDERS TO ATTACK FOR THE FORMATIONS OF THE ARMY ENUMERATED IN THE HEADING .....
.....STAFF OF THE 27TH ARMY 13.6.43 1730 HOURS MAP 1:100 000 NOVOGORJE —
CHIEF OF STAFF COLONEL KLIN"

Prompt recognition of such concrete plans of the enemy for attack or deployment led, particularly in the early months of the war, to some notable successes by the German forces. Thus for example, a promptly recognized order for a large scale Soviet bomber attack on the Düna River crossings called forth German countermeasures resulting in the destruction by German pursuit planes (Moelders) of more than 100 Soviet bombers before they reached the target. The great German success against

a convoy in the Arctic Ocean was likewise due to a promptly decrypted Russian radiogram reporting location, route, speed, and size of convoy.

Recognition of Operational and Tactical Measures: All through the war the decryptment section was able to recognize and report to headquarters preparations for major enemy operations, for example, through the pin-pointing of assembly areas. Naturally this knowledge was not based upon the content of individual decrypted messages but resulted from current observation of events on the individual front sectors, wherein reports of movements of forces played the most important role. In this respect the summoning or bringing up of specialist troops, generally units intended to pave the way for attack, i.e. " ОГМД " ОТДЕЛЬНЫЙ ГАУБИЧНО-МИНОМЕТНЫЙ ДИВИЗИОН (popularly called Stalin Organ) was very suggestive and valuable. The bringing up of reserves, which was often recognized early from decryptments, did not necessarily signify plans for attack but could mean preparation for large-scale operations when other characteristic indications were found.

Recognition of Supply Situation: Of only indirect, but nevertheless by no means negligible value, was the decryption of supply messages from which a fairly clear picture of the enemy's supply situation in individual areas could be drawn. Knowledge of this situation, of available stocks of ammunition and weapons, of gasoline supply etc., sometimes permitted deductions regarding the power of resistance of encircled contingents. The authors recall vividly the almost unbroken intelligence regarding the supply situation of the Soviet forces in the Crimea during the late winter of 1942. At that time decryptment was able to give for almost every single hostile unit the daily changing supply picture as well as the stock of ammunition by rounds of each calibre, the precise amount of motor fuel and of other stocks, and sometimes the replenishments expected.

Example of an ammunition report:

"TO THE CHIEF OF [illegible] OF THE BLACK SEA ARMY.
AMMUNITION STOCKS: 18TH BLACK SEA BRIGADE HAS (MORTAR AMMUNITION) 81 MM - 470, 105 MM - 62, "..." ....ANTI-TANK GUNS) 76 MM -905 RIFLE CARTRIDGES - 18030

ROMANOV"

FF-196

Losses of Men and Materiel: Of similar importance was the decryptment, at times current, of radio reports from the enemy concerning the losses of men and materiel on the various front sectors. In the previously mentioned phase of war on the Crimea, it was possible, for instance, to decrypt such messages almost daily. Such reports were generally part of a message dealing also with other questions, and at that time were in the following form:

Example of a report of losses:

"..... 4. LOSSES FOR 23.2.42: 17TH BLACK SEA BRIGADE — KILLED: SUBALTERNS 3, SOLDIERS 11; WOUNDED: OFFICERS 1, SUBALTERNS 0, SOLDIERS 24; MISSING: SUBALTERNS 1, SOLDIERS 7; KILLED: DRAFT HORSE 1. BURNED OUT 2 T-34. FIRED ON 1.

Since these reports often ended with present strength of men and materiel or were followed at brief intervals by such reports, they yielded a useful picture. Thus the authors recall that the Operation Group "Popov" during its efforts to break through to the Sea of Azov in the spring of 1943 gave in daily reports along with its losses the present strength in greatest detail for each of its units. Since these were intercepted and read, the German command was able to make use of all these details.

Replenishment of Old and Formation of New Units: No less important for our own command was the knowledge of intended or already undertaken reenforcements of hostile units. Such information was often obtained in great detail from decrypted messages. Usually messages announcing the arrival of reenforcements contained valuable details.

Example of report of arrival of reenforcements:

..... SEND ON EVENING 17.4.43 to STATION KOMAROWKA ONE OFFICER AT EIGHT HRS TO TAKE OVER 740 REPLACEMENTS. DISTRIBUTE THESE AS FOLLOWS: OF THE 172 TANK MEN ASSIGN TO 36TH GUARD TANK BRIGADE 48 MEN, TO 174TH TANK BRIGADE 64, TO THE GROUP KUSOV THE REMAINING 60 MEN: OF THE 43 RADIO OPERATORS ASSIGN 21 TO THE 174TH ARMORED BRIGADE, THE REMAINING 22 to 216TH MOTORIZED INFANTRY BRIGADE. OF THE 64 MP RIFLEMEN ASSIGN ALL TO KUSTOV. THE BALANCE OF 461 MEN YOU WILL DIVIDE BETWEEN YOURSELF AND THE 311TH INFANTRY DIVISION ACCORDING TO NEED ....."

The withdrawal of badly battered units from the front and their transfer to rear areas for re-forming, as well as the formation of entirely new units from recruits could often be learned from decryptments. Thus it was possible

to follow the formation of two new armies during the winter 1941/1942 for a time, to learn various details regarding training of the recruits, and — as the most valuable part — to tell the probable time and area of commitment. Deductions from decryption were later factually confirmed.

State of Health and Morale of Troops: The picture of the fighting strength of the enemy troops was rounded out by decryption of radiograms containing details of health and morale of the troops. Reports of this nature appeared particularly in the early months of the war and, since they came mostly from encircled units, were often of an alarming kind. But even when the battle front was relatively stabilized, the political leaders of small and medium units sometimes had occasion to complain of sinking morale or of open dissatisfaction. Noteworthy and important in estimating the fighting spirit of the RKKA was the concern which was manifest in messages all through the war about an obviously strong tendency among the ranks of Red Army soldiers to desert. The attempt was made to combat this by disguising as national patriotism the international-Communist-Bolshevist fighting ideal which elicited little response among the RKKA men. It was possible to follow in the decrypted messages the steps taken systematically to bring about such a change in the thinking of the troops.

Passwords and Recognition Signs: Decryption of messages containing passwords and recognition signs led to local, usually lesser, successes. Such messages often contained recognition signs for several days, sometimes for two or three weeks in advance so that they were very useful to our command.

Example of Message Containing Recognition Signs:

"TO COMRADES OF THE 105TH, 67TH, 26ATH, 301ST INFANTRY DIVISIONS, 16TH AND 107TH ARMORED BRIGADES. SIGNAL FOR RECOGNITION OF OWN AIR FORCE BY ARMY UNITS — "AN OUR PLANE". TO BE GIVEN on 23.5 BY DAY BY TWICE DIPPING RIGHT WING; AT NIGHT 23.5 TO 24.5 BY SHORT BLINKER SIGNALS WITH LIGHTS ON BOARD FOR THREE SECONDS. 24.5 BY DAY DIPPING BOTH WINGS ALTERNATELY; IN NIGHT 24.5 to 25.5 TWO WHITE AND ONE RED ROCKET. ON ...."

Example of Message Containing Password:
"PASSWORD FOR 27.11 CHALLENGE - "TASCHKENT" - RESPONSE - "KASAKSTAN - . FOR 28.11 ....."

DF-196

Situation in Rear Areas: Valuable inferences concerning the situation behind the Russian front could be drawn particularly from decryption of radiograms of the Frontier and Security Troops employed as a security barrier. From this material it was possible to determine that the difficulties caused by German agents — dropped mostly by parachute at night behind the Russian lines — were considerable and called for counter defensive action. Knowledge of the countermeasures taken by the Soviets constantly made possible new methods of introducing our own agents. Appreciable disturbances in the Soviet supply lines were also occasioned by bands of anti-Soviet Ukranian and Baltic elements, and even by small groups of deserters from the RKKA. Knowledge of the existence and activity of such "indirect allies" enabled the German command to incorporate these in their plans and to support materially such groups. The extent of such disturbances becomes apparent from the fact that the NKVD Security Troops often had to send considerable contingents — sometimes several regiments and even operative NKVD divisions — for their liquidation. Thus, for instance, the 18th Cavalry Regiment NKVD was tied up by such action in the southern Ukraine for over four weeks.

To the same category belongs logically information obtained about the activity of spies and saboteurs in Soviet rear areas. It would take us too far afield to cover this; the fact is therefore merely mentioned.

Details on Traffic and Transportation Situation: Important also for clarifying the situation in the rear area was the decryption of messages concerning traffic conditions on Soviet railways, waterways, and roads. Intercepts which were read showed overloading of definite stretches, concentration of transports at certain points, and re-routing of supplies; thus they afforded hints for the employment of the German Air Force and at the same time were helpful in orientating the German command. In the question of overcoming the difficulties of transportation which arose frequently, the will of the Russians was generally recognizable to master these by total and rigorous measures. Thus whole villages, including children, were used to repair supply roads; transport trains were ordered

to run in sight of one another; and sometimes drums of gasoline were rolled by hand from town to town.

Details on War Production: Sometimes, even during the war, it was possible by monitoring single radio nets, particularly of NKVD organs and the АЭРОФЛОТ(Civil Air Fleet), to get valuable insight into the production capacity of individual plants and factories. Thus, for instance, for a long time the capacity for oil production of Makkop, the range of production of several munitions plants in the Crimea and on the Sea of Asov, and the production capacity of some large plants for "SIS-5" (a type of truck) and "T-34" could be followed. Messages of the Civil Air Fleet afforded data on ups and downs of production in armament plants beyond the Urals.

Partisan Activity: With the coming of winter 1942 partisan activity began in German occupied White Russian territory, and spread over almost the entire German supply line. The partisan groups, operating in units of various size , were at first on their own resources, but later were combined into a general partisan organization and their employment was controlled by the USSR. The partisan movement had its own staffs working in collaboration with the front staffs and NKVD organs. Finding and corbatting such partisan groups was possible only by observing and decrypting traffic between the groups and their staffs.

Infiltration of Reconnaissance Groups and Agents: Similar partisan command organizations also controlled the infiltration of reconnaissance groups and agents into the German rear areas, mainly by means of parachuting from airplanes. Here also it was the task of decryption to make possible the location of these groups.

Polish Resistance Movement: In the last phase of the war abundant traffic could be intercepted and decrypted affording ample information about a National Polish Movement and its activities. From the content it could be inferred that this movement at first assumed a waiting attitude toward the Soviet Union and took its instructions directly from London.

It was clear that the organization which was then in its infancy was pursued by the NKVD organs, as was apparent from the numerous reports of successful arrests of its members by the Russians. There were also repeated complaints concerning acts of terror on the part of the NKVD.

Significance of Cryptanalysis: The examples given probably show fairly clearly the significance of a cryptanalytic unit. Operated systematically and regularly, it yields in peacetime important information concerning developments in various fields of life in the country observed. Often from these observations valuable conclusions can be drawn about the true intentions of the state — intentions which may otherwise be more or less skilfully camouflaged. The value of decryptment during a war is obvious. It warns one's own command by giving it the enemy's plans; it makes possible reasonably safe dispositions by revealing the position and strength of the foe; and it shows weak spots as well as worthwhile objectives for attack.

To a certain extent decryptment eliminates uncertainty and hence risk in connection with military operations. It is perhaps the youngest, but already a rather acute weapon whose value when employed on ample scale must not be underestimated either for defense or offense.

PART II. TECHNICAL

A. The Russian Cryptographic Service.

Its Structure and Organization

Army and Air Force, 8th Section of General Staff of RKKA and its Subordinate Organs: The highest authority and thereby the guiding agency for all matters concerning the cryptographic work in the Army and Air Force of the USSR is the 8th Section of the General Staff of the RKKA in Moscow. Directly subordinate to it are all 8th Sections of the front staffs, armies, and corps, and all 6th Sections of the divisions and brigades as well as the "ШО" - ШИФР. ОТДЕЛ = crypto sections of the lower formations. The 8th Section in the General Staff is divided, according to its duties, into three groups, each of which assumes a number of functions.

Organization of the 8th Section of the General Staff of the RKKA in Moscow.

Group 1: Personnel matters

Issue and recall of cryptographic materials for the Army and Air Force

Preparation of cryptographic material

Recording of all encrypted messages in operational and tactical systems (5-digit)

Group 2: Development of mechanical aids

Development of cipher machines and testing of proposals in this field (Baudot, secret teleprinter, etc.)

Group 3: Employment of РАДИОРАЗВЕДКА = radio intelligence

Cryptanalysis

Evaluation

DF-196

Basic Changes During the ... up to Spring 1945: In the selection of communications personnel, in particular those dealing with cryptologic material, extraordinarily strict standards were applied until the beginning DF-196 of 1942. It was repeatedly stated by prisoners and was confirmed by captured material that all those engaged in the 8th Section or its subordinate organs, even down to the last "ШО" co-worker in the smallest unit, had to be old Party members and absolutely reliable in their political attitude. The selection of this personnel was therefore completely under the control of the NKVD. Likewise the two special schools for crypto personnel in Moscow and in Tambov were conducted by the NKVD. The period of training at these schools before the war and down to the beginning of the year 1942 was six months; in addition to the handling of the most varied cryptographic systems, the history of cryptography was taught in condensed form and the field of cryptanalysis was touched on briefly. After the heavy losses in the summer and fall of the year 1941, which were felt also among the crypto personnel, they were forced to change the regulations in respect to selection and to reduce the training time in the schools. Since 1943 non-members of the Communist Party can be employed as cryptographic workers; the training time, which was first shortened to three months, has been only one month since 1943. Because of the heavy losses of men, the personnel strength of the 8th and 6th Sections had to be sharply reduced and the heavy losses of officers in particular resulted in the employment of civilian officials as directors of the 6th Sections with brigades and divisions. In general it may be stated that the strength was reduced at that time by approximately 35 percent and that civilians of equal grade or junior officers took over the conduct of the 8th and 6th Sections.

Since reductions in strength and in the period of training at that time doubtlessly occurred in other parts of the communications service, it was understandable that the performance and reliability of radio operators and crypto clerks could not fail to suffer and consequently more errors occurred in encrypted messages which often rendered decryption much more difficult. Frequent inquiries on many Russian links, requests for repetitions or for changes of key proved that the difficulties were

noticeable in their own operations. These facts were doubtlessly one of the reasons for the speedy development of Baudot links in internal traffic, since this made it possible to economize on communications personnel inside the country. Whether in addition to Baudot and secret teleprinters cipher machines were also put into use on other internal lines has not been determined absolutely; it can be stated, however, that traffic in machine systems has not appeared as yet on military links. One cannot avoid the impression that the Russian prefers manual methods of encryptment, all the more so since he has found in the use of the one time additive the ideal method of reencipherment.

According to several statements by prisoners, deserters, and agents, Russian radio intelligence stressed primarily the results of direction finding and operational and traffic analysis, while ostensibly decryptment was able to achieve only scant results despite extensive employment of the 8th Section in Moscow. Radio intelligence represented in any case only a very unimportant and little developed part of the Russian communication service. Only a few front staffs had their own units for radio intelligence whereas from the army down to the division only individual intercept receivers and direction finders served these purposes.

The preparation and issue of new cryptographic systems as well as the withdrawal of those replaced was until early 1942 exclusively the duty of the 8th Section of the General Staff in Moscow. In this way a unified direction and control was possible and the issue of only a few general systems afforded the advantage that these were thoroughly mastered by the cryptographic personnel and that errors in ecryptment could generally be avoided. After the first few months of the war between Germany and the Soviet Union the necessity already became apparent for carrying out fundamental changes in respect to the preparation and distribution of cryptographic systems.

DF-196

The rapid German advance during the summer and fall of 1941 had as a result that in the great encirclement battles, in connection with unforseen flank and pincer movements numerous Soviet cryptographic documents of the Army and Air Force fell undamaged into the hands of the German troops. Since when cryptographic systems were in general use the capture of a single copy was sufficient to compromise the system of the entire front, it was obvious that the Soviet High Command had to make a change as quickly as possible. This basic shift in the organization of the cryptographic service during a period which was extremely critical for the USSR, was made, using the threat of heavy penalties in case of delay or contravention, in the notably brief time of three months and had been completed everywhere by the end of March 1942. In contrast to the centralization in time of peace, the production and distribution of cryptographic material was now decentralized. Only the production of the operative and tactical 5-place code (Chiffre) was still reserved to the 8th Section of the General Staff in Moscow, while the front systems - called since then "СУВ = СКРЫТОЕ УПРАВЛЕНИЕ ВОЙСК - camouflaged transmission of messages of the command - were worked out by the signal officers of the immediately superior units, were issued at their discretion and, were likewise replaced when there was danger of compromise. The systems which resulted were distributed to the formations and to the neighbor organization - from left to right. For the setting up and working out of "СУВ systems by the individual signal officers a scheme was worked out by the 8th Section of the General Staff which outlined in a general way the size and type of such cryptographic systems but contained no directive regarding the choice of the reencipherment.

The Russian owed it solely to this change in the organization of the cryptographic service that the readability of his army messages became much less and that the capture of such cryptographic systems no longer represented a danger to the entire front. The multiplicity of these systems, the slight amount of traffic on the individual net and the short

period of use - particularly in the army, rade analysis extremely difficult and rade dealing with small groups of messages an impossibility. If it was possible, nevertheless, right down to the final days of the war, to provide the High Command with important information, often when our own communications were very difficult, that was due exclusively to the fact that the former German Army had enough trained and experienced cryptanalytic personnel.

Chart of the General Types of Cryptographic Systems

— Size and Area of Use —

Army and Air Force:

Type Designation	Size (groups)	a.	b.	c.	d.	e.	f.	g.	h.	i.	j.	Remarks
Chiffre	10000 - 25000	+	+	+	+	+	+					
Code	3000 - 10000			+	+	+	+	+				Not in use
Code table	2000 - 3000											Not in use
"CYB"	500 - 2000			+	+	+	+	+	+			
ПТ	100 - 500								+	+	+	

NKVD:

Type Designation	Size (groups)	k.	b.	e.	l.	g.	h.	m.	n.	o.	p.	Remarks
Chiffre	10000 - 25000	+	+	+	+	+						Chiefly economic messages
Code	3000 - 10000	+	+	+	+	+						
Code table	2000 - 3000			+	+	+	+	+	+	+	+	
"CYB"	500 - 2000			+	+	+	+					
"ПТ	100 - 500					+	+	+	+	+	+	

Explanation:

a. General Staff
b. Front Staff
c. Army
d. Corps
e. Division
f. Brigade
g. Regiment
h. Battalion
i. Company
j. Platoon
k. Группа
l. Unit (Abteilung)
m. Field Posts
n. ОЧГ
o. ОПЕР. ГРУППА
p. МАН. ГРУППА

At the conclusion of the section dealing with the cryptographic systems of the Army and the Air Force the conjecture may be expressed that the 8th Section of the General Staff in Moscow may return with the end of the present war to centralization of the development and issue of cryptographic material. The authors see arguments for this in the fact that, in the first place, a direction and control of the vast apparatus is much simpler in this way and, in the second place, in the reflection that the sole reason for the change in 1942 - the possibility of the capture of secret documents by the enemy - drops out. This shift would be very important for cryptanalysis, in particular because, assuming a longer period of use and consequent larger traffic receipts for a system, it would permit devoting careful attention to the structure of the system and make possible the supplying of completely deciphered messages rather than merely a fragmentary reading.

NKVD Guidance and Control of NKVD Cryptographic Systems: The central office for the cryptographic service of the NKVD organs is located with the Г/П НКВД in Moscow. Organization and functions of this section in the field of cryptology are not known. In contrast to the cryptographic systems of the Army and the Air Force, it has not been possible in any case to capture NKVD systems which were still in use. At various points on the front 4-place NKVD codes have fallen into the hands of German troops, but either they were then no longer in use or they represented reserve systems which, due to their capture, were not put into use. On the basis of what has been said above, the NKVD cryptographic central office was able to retain the method of centralization for the production, issue, and recall of cryptographic material throughout the entire war. Consequently, in spite of the great number of different NKVD organs, there was only a very limited number of NKVD cryptographic systems in use and it was also true that these were valid for a relatively long time, often more than two years. In consequence it was possible for our own cryptanalytic units to do extensive work on these systems and eventually to read the NKVD messages 100 percent. One must not make the mistake, however, of regarding the NKVD systems as simple and easily decipherable;

on the contrary, from the very beginning they have been very resistent to systematic cryptanalytic effort and the fact that they could be read completely in the end is due solely to the long periods of use and to the untiring diligence of those who worked on them.

Brief Survey of Intra-state Circuits: The monitoring and decipherment of internal radio traffic was not a duty of the Army signal intelligence agencies; nevertheless of necessity systems used on internal networks were in part worked on and solved. Special units were devoted, among other things, to the reception of Baudot traffic but here the value of the evaluation results lay almost exclusively in the economic field. This much did become known: all this traffic was not merely controlled by the NKVD but in many cases was directed by the NKVD and in all probability the "[illegible] НКВД was also responsible to a great degree for the issue of cryptographic material for internal radio traffic.

Partisans, Agents, Scouts: The NKVD also had an important share in the preparation and issue of cryptographic materials for partisan organizations and for the agents and espionage service. In view of the initial multiplicity of partisan groups which operated independently and of the often very extensive employment of agents and spies in the enemy's rear, it was necessary to provide for current replacement of cryptographic systems, in which connection it was of primary importance that these should be convenient, simple to use, and secure. This responsibility could not be met by a single central unit, however large; therefore the individual partisan staffs, which for the most part were located in the immediate vicinity of Army front staffs, were assigned the task of producing and distributing such cryptographic systems, although all of them were subject to the guidance and control of the NKVD.

From the foregoing observations it is clear to what an extent the NKVD apparatus influenced the requirements of the Army and the Air Force as well as communications in the economic field. Especially noteworthy is the high degree of training and the sense of responsibility of the

NKVD personnel which made it possible to prevent any cryptographic systems of the NKVD which were still in use from falling into the hands of the enemy during the entire period of the war.

B. Development of Russian Cryptographic Systems in the Light of Cryptanalysis

Army and Air Force Systems: The relatively high level of Russian decipherment in the former German Army was to be ascribed primarily to the fact that systematic observation of Russian radio traffic and hence, too, cryptanalytic work was begun promptly. The development of the Russian cryptographic service has shown precisely how important it is to start analysis of the encrypted messages of a country, if possible, at a time when the cryptographic work of that country is still primitive. Then, however, it is necessary in any circumstances that monitoring of the traffic shall not be interrupted even for a short time, since otherwise one's own cryptanalytic unit cannot keep step with the development of the keys and so of the cryptographic systems of the country under observation. In the case of Russia the former German signal intelligence service had succeeded in fulfilling all prerequisites for a favorable development of Russian decipherment; the following historical cryptographic review will supply the best proof of this.

At the start, it may be mentioned briefly that no rule can be given for cryptanalysis itself, that is for the general ability to force unknown cryptographic systems and to make them readable. The ability to cryptanalyse will always depend on a certain aptitude and a good general knowledge; linguists and mathematicians balance one another in this matter. Of course the analyst makes use of many traditional pieces of information such as the frequencies of letters, digraphs, trigraphs, and syllables, while mathematical principles of combinatory analysis, the theory of series and probability all find application. Nevertheless an acquired

knowledge of all these details will never be able to supplant the intuition of a good cryptanalyst.

For specific reasons, but primarily to avoid a confusion of technical expressions or concepts, in what follows the individual types of systems will be treated successively.

Operational Systems: Under the heading "Operational Systems" fall all those cryptographic systems which are conceived primarily for operational and technical transmissions. Some short messages of this kind may be given as examples:

"OUR RADIO STATION WILL WORK TOMORROW FROM 0700 - 1100 HOURS AND FROM 1500 - 1900 HOURS. LEVTSHENKO."

"WHY DO YOU NOT ANSWER OUR CALLS? OUR WAVE IS 157"

"TO THE HEAD OF THE RADIO STATION. YOUR OPERATORS ARE PERFORMING BADLY, SEE THAT THEY ARE REPLACED. CHIEF-SIGNALS".

All systems of this kind - they are almost always substitutions (Cäsaren) and in rare cases small codes - bear the designation "ПТ " = ПЕРЕГОВОРНЫЕ ТАБЛИЦЫ = chatter tables. The first operational system, used for a long time by the Army and the Air Force of the entire Soviet Union was the "ПТ -35" (chatter table of the year 1935). It contained 100 groups and was reenciphered in a different fashion almost daily on the individual nets (See Plate 1).

The 10 x 10 number squares serving as key were known as "system squares" and rendered the cryptanalysts and especially the content evaluators valuable service toward identification of traffic. In general at that time three or four system squares were employed simultaneously in one military district and they remained in use for as long as two years. Hence it was quite possible, and was repeatedly observed, that keys which had once appeared were used again after a reasonable time.

In the final months of 1939 the "ПТ -35" was replaced by the "ПТ-39". This operational table, in contrast to the preceeding, had double entries in part and contained two indicator cells which showed the method of

DF-196

reading. The type of reencipherment was the same, save that the system squares were changed more frequently (See Plate 2).

With the beginning of 1942 the "ПТ-41" came into use as successor to the "ПТ-39". With the same size as its predecessors (10 x 10), here 98 of the 100 cells had two meanings; two indicator cells showed the method of reading to be used. The alphabet and the digits 0 - 9 were all assigned two groups; the most frequent letters: O, И, E, Н, Т, A, B, C, P, K and a few others had three groups. The reencipherment by the aid of system squares also remained the same, merely that there was a more frequent change, sometimes monthly (See Plate 3).

The receipt of radiograms enciphered according to the operational systems was very high from almost all military districts, later front sectors, down to the end of 1943. In 1944 the receipt of messages of this type grew less from month to month; to make up for that other operational systems - partly small codes - appeared which were used, however, only in limited ranges. The reading of these essentially simple systems was not always easy in view of the very light traffic receipts. The structure of such codes corresponds in essence to that of the systems described a few pages later on under the heading "Substitution Systems".

In regard to the operational substitution systems we may say in conclusion that almost always 2-place cipher groups are involved - horizontal and vertical coordinates - which in the cipher messages were combined in 2- or 4-place groups.

Signal Tables: "Signal Tables" did not appear in the cryptographic picture of the USSR until the second half of the war. These are 3-and 4-place systems of slight size which fall under the designation "СУВ" and are used exclusively in tank units. Aside from a spelling alphabet they contain only 1-digit numbers and words which are important for tank warfare. Unimportant words are sent in clear in messages of this type; map coordinates - usually 5-place - are disguised according to map keys. A message enciphered by a signal table would look somewhat as follows:

DF-196

ПРОТИВНИК	СИЛОЮ		1	БАТАЛЬОНА	НАСТУПАЕТ		
2734	4659	ДО	7143	6275	1485	ИЗ	
РАЙОНА					СЕВЕР		
8119	27345	27452	27461	НА	4038	-	

Translation:

"THE ENEMY IN STRENGTH OF ONE BATTALION IS ATTACKING TOWARD THE NORTH FROM THE AREA (LOCATION IN ENCIPHERED COORDINATES)."

Linguistically perfect solution of such tank signal tables was possible only in the rarest cases; frequent change of key and often slight traffic receipts rendered cryptanalysis much more difficult. Nevertheless, in most cases even a fragmentary reading can afford important clues.

Address Codes: Since in general addresses and signatures spelled out or in the form of syllables-afford one of the most important points of attack for hostile cryptanalysis, the Russians in 1943 began enciphering the addresses and signatures in messages enciphered by the "CYB" systems using a special address code independent of the rest of the text. These supplemental codes, issued independently by the front or army units, contained in addition to such simple concepts as "Chief", "Commander", "Leader", or "Deputy" composite concepts like "Chief of Staff", "Head of the Radio Station", "Chief Signals" and in addition in the case of address codes in an army unit expanded aggregates like "Commander of the 17th Tank Brigade", or "Chief of Staff of the 231st Infantry Division". Interpretations, especially of this last type, were hard to make and could only be achieved after careful, intensive observation of the traffic concerned. Especially difficult was the solution of reencipherments of such address codes. Nevertheless, despite the difficulties, even here good results could be achieved.

Substitution Systems: The greatest number of decrypted Russian systems belong doubtlessly to the category of substitution systems including codes, code tables, small and very small codes and expanded substitutions. Systems of this sort have appeared in Russian cryptography since observation began and even though, compared with the present state of Russian cryptography,

they must be designated as very primitive, it is worth while to outline them (See Plate 4).

The reencipherment extended only to the ten pages, each of which could be expressed by from two to ten different dinomes, while the basic numbers of the groups remained unaltered. Change of reencipherment resulted irregularly and at different times in all military districts or nets. The general Air Force code represented schematically was used in the years 1934 to 1937. Other Air Force codes of like type appeared annually around 1 May and remained in use for a short time, approximately for one month. These systems were used for practice in connection with the maneuver-like air parade on 1 May in Moscow. Starting and landing reports, weather reports, operational messages of the air units arriving from all parts of the Soviet Union to participate in the parade were enciphered with these. These were regularly 3-place systems with some 500 groups and an absolutely alphabetic structure. Reencipherment was by single digit substitution for the three elements.

Aside from a number of small and very small codes, which were used for a short time during various maneuvers and exercises of the Air Force in all military districts, the last Air Force system of this kind, the "BAK-38" = ВОЕННЫЙ АВИАЦИОННЫЙ КОД 38 ГОДА = Air Force code of 1938, is especially worthy of mention. This 3-digit code comprising some 800 groups contained letters, words (no syllables!) cover groups for airplane types, numbers, marks of punctuation, and composite concepts such as "AIRPLANE ..... HAS MADE EMERGENCY LANDING." or "AIRFIELD UNSUITABLE FOR LANDING". This system could be transmitted with one of three basis encipherments which were designated by the colors "black", "red" and "green" and which were reenciphered by digraphic substitution of the "ab" elements of the groups. Element "c" remained constant within the basic encipherment (See Plate 5).

DF-196

This system, which was in use from 1938 to the end of 1939, represented a great advance over its predecessor. From this time on systems of this type no longer appeared as general systems of the Soviet Air Force.

In contrast to the Air Force which had known such systems since 1935, a generally used system did not appear in the Army until 1937. Before that a relatively large code for exclusive Army use was known only in the military district of Moscow. The code which appeared here contained 20 pages with 100 groups each and was therefore more than twice as extensive as all Air Force codes known up to that time. It was terminologic-alphabetic in structure with 4-digit groups and roencipherment of the elements "ab" was by dinomial substitution, element "c" by single digit substitution, while element "d" remained unchanged.

Since an exact description of each individual known system, even of the larger ones, would be too much of an undertaking, only one of the best known 4-place combined Army and Air Force codes will be described in detail.

The first general Army and Air Force code of considerable extent was the 4-place code with some 4600 groups which appeared initially in connection with maneuvers in the Volga military district. Reencipherment of this code and of all of its successors - codes "OKK-5" to "OKK-8" - was by means of dinome substitution series or tables for the elements "ab" and "cd" of the code groups. Two indicator groups showed in each instance the series and the starting points therein. The "OKK-5" = ОБЩИЙ КОМАНДИРСКИЙ КОД-5 = General Commander Code - with 50 pages of 100 groups each was compiled with such extraordinary technical skill that its successors showed only slight changes when compared with it. The use, i.e. the swift succession of four great codes in the course of the years 1939 to 1941, is explained only by the fact of their capture - "OKK-5" in the Finno-Russian war, "OKK-6" to "OKK-8" in the German-Russian war. All these systems had been recovered, however, and were completely read currently even before their capture (See Plate 6).

DF-196

The last substitution of large size used was the "ОЦКК-7" = ОБЩИЙ ЦЕНТРАЛЬН. КОМАНД. КОД= General Central Commander Code - which was used in the interior and afforded very valuable clues regarding replacements and new formations of the enemy. Its reencipherment was by dinomial substitution tables similar to those of the previously described systems.

To the category of substitution systems belong without exception all systems coming under the designation "CYB". After the decentralization of the Russian cryptographic service had been carried out, the fact that the signal chief of every division, indeed of every regiment, could compile and develop systems of his own for his own area gave great latitude to the fancy and initiative of each individual. Apart from numerous extravaganzas (Stilblüten) in the construction of "CYB" systems, particularly in the beginning, finally some proposals resulted which had to be taken seriously and represented important increases in security when compared with the earlier small substitution systems of this kind. Above all else the fundamental change from a single reading to a double reading materially limited the possibilities of cryptanalysis and today considerable quantities of traffic are necessary in order to force a break-in. The double reading of a system consists in including 2, 4, 6, ... 20 switch groups (Hinweisgruppen) in the system, half of which signify "READ THE ENTIRE WORD" (the complete meaning), the other half: "READ THE FIRST LETTER OF THE WORD". In this way it has become possible to use each word under a given letter as a single letter element. Thus it is possible to dispense with the auxiliary alphabet which had been usual up to that time. With this the frequency peaks of individual letters "I" or "C" were flattened.

The great number of "CYB" systems which varied greatly in extent and structure makes it impossible to describe them individually. Once more it will suffice to indicate that of all the changes the introduction of the double reading is the most important and most fundamental.

DF-196

Transposition Systems: Pure transposition systems, e. g. boxes, have appeared in the Russian Army and Air Force only for practice use, and as training for a link planned in 1937 between the Soviet Union and Czechoslovakia. The content was pure propoganda text.

For the transmission of radio messages of operational or tactical content, i.e. dealing with troop command, on the nets of the upper and top command (from brigade or division staff upward to the General Staff of the RKKA) the 5-place "Chiffrecode", also called "Operational Code" was used as a matter of principle. The "Chiffrecode" or for short the "Chiffre" was systematically adapted by the Russians in the course of years to the changing requirements of their vocabulary and was improved in respect to security against cryptanalytic attack by more and more consistent use of variants for the most frequent groups (marks of punctuation). These new editions of the "Chiffre" came during the war at intervals of 6 to 12 months, whereas in peacetime the same code was used much longer. At the beginning of the German-Russian war code "011-A" was in use which was then replaced by code "023-A", "045-A", "062-A" and finally by code "091-A" which remained in use until the capitulation of Germany. All these codes, except "045-A" which was in use from March 1942 to March 1943, were alike in structure - aside from the above-mentioned progressive improvements and amplifications. They were divided into the general part with vocabulary in terminologic-alphabetic order and the "special part". The general part contained letters, digraphs, trigraphs, syllables, words, phrases, and entire sentences arranged in strictly alphabetic sequence, with the marks of punctuation, fractions and ordinals, hours and minutes, numerical designations of armies, corps and divisions, day dates, year dates, and calibre designations scattered throughout the entire code. In the special part these concepts, which had been entered out of alphabetic order, were brought together once more in numerical order to facilitate looking up these concepts in the code by the code clerk. Code "011-A" embraced some 19,000 groups which were entered

on some 390 pages; the systematic development of the code resulted in an increase in the number of groups with each new edition. The last known code "091-A" had some 23,000 groups on 430 pages. In spite of the relatively unimportant expansion of the code, the improvement was very considerable from the standpoint of the cryptanalyst. The main point of attack for the cryptanalyst is afforded by the frequency peaks occurring in the text and conditioned by the language itself, these are primarily the marks of punctuation (period and comma which with some 6.5 percent and 4 percent respectively stand at the top of the frequency curve of Russian military messages with the type of contents found in the Chiffrecode). While these concepts still had only one group each in code "011-A" and thus afforded the analyst a good chance to break in, the number of variants increased with each new edition of the code and in the final edition "091-A" reached a total of some 230 groups for each of these two marks of punctuation. Thus the analyst was forced to change utterly his method of breaking in and to employ much more round about means.

As already mentioned, code "045-A" fell out of the ranks of the terminologic-alphabetic codes. This code showed interrupted alphabetic structure. To a practiced cryptanalyst this hardly caused greater difficulty. It is interesting to note that, while all new versions of the Chiffrecode during the course of the war were always captured by good fortune so early that the originals were almost always in the hands of the cryptanalyst by the time they were put into use by the Russians and consequently there was no necessity for code recovery, precisely the more difficult code "045-A" did not fall into German hands until some three months after it had been put into use in the RKKA. In these three months, however, it had been so far recovered by our cryptanalysts, in spite of the essential departure from the structure of its predecessors, that it was already possible to read currently some part of the messages encrypted by it.

Additive Systems: The loss of the Chiffrecode, even its capture by the enemy, is not considered important by the Russians because they take the attitude that the method of reencipherment applied to messages encrypted by the Chiffrecode affords complete security, even when the code itself is in the hands of the enemy. This method of reencipherment consists in applying to the 5-place code groups 5-place additive groups from a practically endless, unsystematically constructed additive numerical sequence (so-called Gamma Tables). The tables used to reencipher the Chiffrecode can be divided according to the manner of their use into two categories: first: the general table containing 300 5-digit additive groups. At the top and at the side of the table are entered 2-digit column indicators and 3-digit row indicators which allow the encipherer to indicate according to the principle of coordinates the additive group with which he begins his reencipherment. Hence in general tables reencipherment can start at any point in the table but must then continue serially until the last text group has been reenciphered;
second: other tables, which bear different designations according to the area of use but are the same in the way they are used. In these tables, which embrace 60, 80, 100 and 120 5-place additive groups, the reencipherment must always start with the first additive group in the table and then continue serially.

The general tables are used for one day in the area of a unit and its subordinate formations (e.g. for the traffic of a front staff with its associated Army staffs, or of an army with its divisions and brigades). The purpose of using such tables is the dispatching of messages the content of which is to be available simultaneously to several recipients (hence the designation "GENERAL"). All other tables serve merely for communication between two partners: the army and one of its divisions, the front staff and one of its armies, etc. These tables, which for this reason are designated "INDIVIDUAL" tables, are to be used only once, in contrast to the "general" tables which can be used several times during one day, because in the latter case security is afforded by the possibility of

using different starting points. The individual tables bear different designations corresponding to the area of use, e.g.: "AKORD" (army-corps-division), "FAK" (front-army-corps), "OC" (special) and "CIRCULAR". Cryptanalytically they all belong to one category - the individual table, since they are all intended only for one-time individual use. Because of the one-time use of each table the demand in the RKKA for these means of reencipherment is extremely great. The production of these tables is in the 8th Section of the General Staff of the RKKA where they are put together in "Blocknots" - the "GENERAL" containing 31 tables each, the "INDIVIDUAL" having 50 tables each - and are delivered to the front staffs. These provide for the further distribution to the army staffs which pass them on to their divisions and brigades.

Worthy of note is the observed shift from the "GENERAL" to the "INDIVIDUAL" tables, because the latter afford almost absolute security against cryptanalytic attack.

NKVD Cryptographic Systems: Operational Systems:

In contrast to the Army and Air Force, which down to 1934 always had only one general operational system current, the NKVD organs, especially the individual border guard districts, almost all had their own operational system earlier. Plates 7 - 9 show the structure and the manner of using such systems. Not until 1939 was a common substitution (Caesar) introduced as operational system for all NKVD organs, similar to the use in the Army and Air Force.

Substitution Systems: Major substitution systems of the NKVD appeared much earlier than in the Army and Air Force. The first, a 4-place code of some 25 pages with 100 groups each, was in use from 1936 on in the border guard district Kasakstan where the border guard was completely cut off especially in winter through frequent destruction of telephone and telegraph lines by snow storms and which received news reports encrypted in this code. This system was reenciphered by a dinomial substitution for the pages of the basic code which changed about once a week.

FF-19%

The three 4-place substitution systems which appeared down to 1939 and had up to 5000 groups were reenciphered by dinomial substitution series or tables, just as in the army. It is worth mentioning that one of these substitution systems, with some 3500 groups, represented a so-called reserve system and appeared sporadically in all possible districts down to 1943 whenever other cryptographic materials were lacking.

In 1939 the first general NKVD code with 10,000 groups, 100 pages with 100 groups each, was put into operation. This was reenciphered initially by digit for digit substitution and later by additive (See NKVD-Additive Systems).

Reencipherment by single digit substitution sequences:

	0	1	2	3	4	5	6	7	8	9
A	7	9	3	4	1	0	8	2	6	5
B	3	6	1	8	7	2	9	5	0	4
C	0	4	6	5	1	3	7	9	2	8

(Basic Code)

Basic code group:	3512	4278	9310	6264
Division:	ABCA	BCAB	CABC	ABCA
Reenciphered text:	4243	7620	8460	8171

At the time of the capitulation three 4-place substitution systems of the NKVD Border Guard and Security Troops were in use and up to 200 messages in these systems could be read daily through cryptanalysis. These involved code tables with 2,000 to 2,500 groups of which 3EPH0 and "H/RA were reenciphered by dinome substitution and "B/3A by dinome and monome substitution. For work with "3EPH0 " each of more than 30 different nets had 20 substitution tables for reencipherment, 10 each for the page and the group. With 10 different possibilities of shifting with respect to one another the group cells on the individual pages, a total of $10^3 = 1000$ different reencipherments could be used. An indicator group, differently placed on each network, showed by its elements "a", "b" and "c" the reencipherment of the group, the displacement and the reencipherment of the page. Element "d" of the indicator group was blind, generally a null (See Plate 10).

DF-196

The reencipherment of code table " НИВА " was similar and was indicated by an indicator group whereas with table " ВИЗА "the reencipherment was less complicated but, to compensate for that, had no indicator. The reencipherment tables were changed within the network as a rule after one to three months.

As the last major substitution system of the NKVD organization may be made of the 5-place NKVD railway code which contained 2500 groups on 25 pages. Reencipherment was by dinome substitution sequences for elements "ab" and "de" and single digit substitution for element "c". This system was in use down to the day of capitulation.

Aside from the major substitution systems described other smaller codes, mostly 3-place, were deciphered and read from time to time, among others one used by the NKVD Escort Troops (Begleittruppen). All these systems exhibit the same structure as systems of like size in the Army and Air Force.

Transposition Systems: Letter transposition such as appeared with the Army for practice purposes could not be identified in NKVD traffic; however, a transposition as reencipherment in connection with a 4-place 10,000 group code was known in the Arctic area and along the Finno-Russian frontier. The system was broken and could be read in fragmentary fashion.

Additive Systems: In the reencipherment of all major codes, including the NKVD, the additive sequence, which first appeared here in 1940 and has since been used with all sorts of variants, plays the major role.

The first additive used as reencipherment for a 4-place code listed among the NKVD substitution systems and originally enciphered by 1-place substitution sequences, was compiled with the aid of a letter substitution table from the book "History of Leninism" by Stalin.

DF-196

Scheme of the letter-digit substitution:

И, З, Щ	- Ø	В, У, Ш	- 5
О, Д, Ф	- 1	С, П, Ы	- 6
Н, Ж, Ц	- 2	А, Г, Э	- 7
Т, М, Й	- 3	К, П, Ч	- 8
Е, Б, Х, Ю	- 4	Л, Ь, Я	- 9

The letters of the text were converted into digits by the above scheme; the starting point was given as an indicator group by naming the page (01 - 99) and the line (01 - 45).

In like manner in 1942 another NKVD code of Interior Troops was reenciphered. The basis for the production of the additive was then a military instruction book "Radio Communications".

The Border Guard Troops NKVD along the frontiers of neutral countries produced their additive, so far as the writers recall, by 20 + 4 numerical sequences, the displacement of which in respect to one another was expressed by means of an indicator group.

The use of double additive recently and down to the day of capitulation (single additive until the end of 1944) making use of Gamma Tables concludes the current development of the additive encipherments of NKVD systems. Here there was a decidedly clever camouflaging of the indicator groups which it was very difficult to detect and which could only be clarified relatively late. The camouflaging of the indicator group was accomplished by different formulae on each net.

Formula: A1 - A4 = S5 + S3
Note: A4 signifies the fourth group from the beginning.
S5 signifies the fifth group from the end.

Message text: 2739 1825 7930 8221 1975 6308 .... 4199 1537 2811 3061 6275
2649 2314 5539 .... etc. 0185 -

Indicator group: 2739 - 8221 = 4518
Control group: 1537 + 3081 = 4518

A1 and S3 are inserted groups (without significance in the text), which are indicated by the final group.
Final group: 0185 (abcd), where a + b show the position of the first, c - d that of the second inserted group.

DF-196

Since in the case of double additive, just as previously with single additive, the same Gamma Tables were used several times; the reencipherment could be removed from 50 - 75 percent of all messages and the content, after recovery of the two non-alphabetic codes which were enciphered with such an additive, could be read down to the day of the capitulation.

In conclusion it must be stated that the high level of analysis of these NKVD systems, which were mostly very difficult, is to be ascribed to the fact that the work was done at a central location, i.e. exclusively in the cryptanalytic signal intelligence agency of the Army and hence increased secrecy was guaranteed. From the mere fact that NKVD systems often remained in use for more than two years it must be adduced that the Russians considered reading by the enemy impossible.

Partisans, Scouts, Agents: Especially varied in their construction are the cryptographic systems of the partisans, agents, and scouts. In contrast to the Army, Air Force, and NKVD, numerous transposition systems come into the picture here, generally single and double box, in rarer cases grilles (Raster). It would take us too far afield to describe all types which were recognized and deciphered, hence we shall take up only the most usual and most characteristic. First and foremost we shall refer to the simple substitution (Cäsar) using both monomes and dinomes and formed with a key word.

Key word: 6 1 4 5 3 2 7

C A M O Л E T (airplane)

А-1, Б-81, В-81, Г-82, Д-83, Е-2, Ж-84, З-85, И-86, К-87, Л-3, М-4, Н-88, О-5, П-89, Р-90, С-6, Т-7, У-91, Ф-92, Х-93, Ц-94, Ч-95, Ш-96, Щ-97, Ъ-98, Ы-99, Ь-00, Э-01, Ю-02, Я-03, (-)-04, (,)-05.

Plain text: Я РАНЕН КОНЧАЮ РАБОТУ.

Translation: AM WOUNDED, FINISHING THE WORK

Enciphered text: 02901882838758895101901805717980З -

The enciphered text can be divided into digit groups of any desired length; it can also be sent in reverse order.

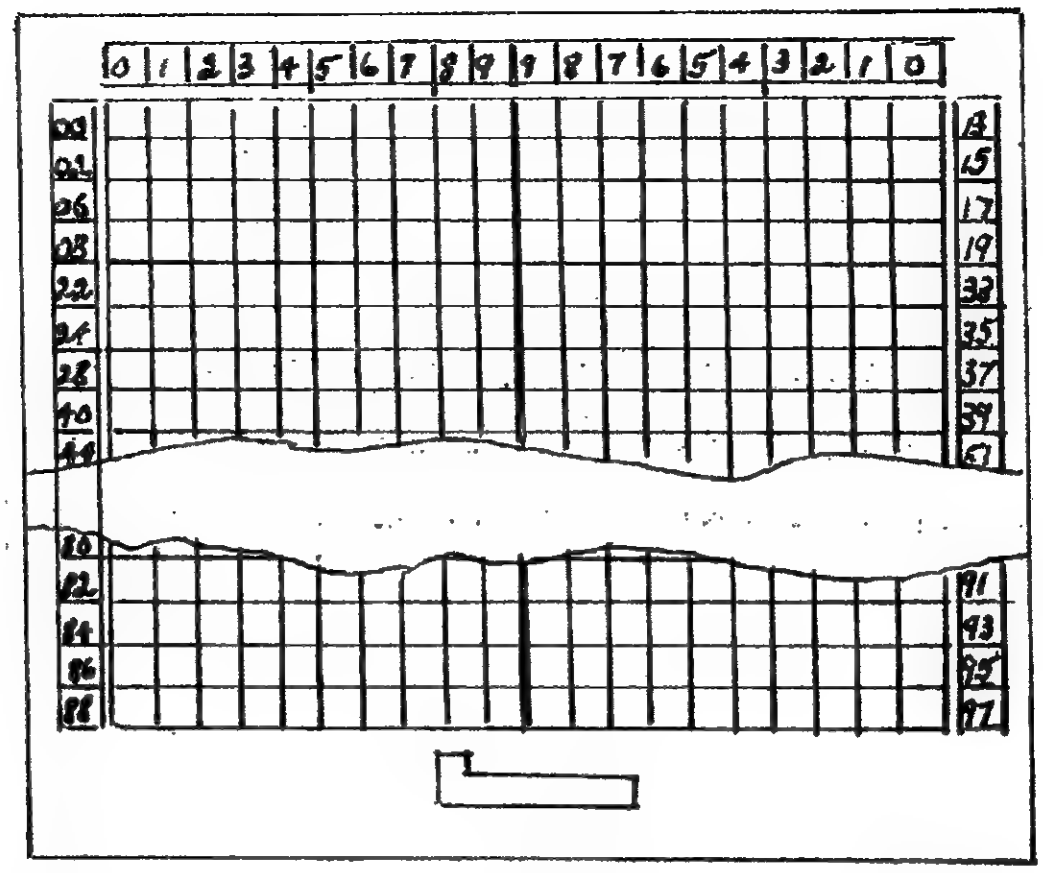
In many cases simple substitutions of this type were transposed or treatment with additive before being transmitted. For the layman a monodinome substitution presents an almost insolvable problem but the frequency count of the individual digits shows with certainty the elements used as tens.

The following types of cryptographic systems, listed according to substitution, transposition, and combined systems, appeared repeatedly; some were decrypted and read:

Substitution	Cäsar Small code
Transposition systems	Box Grille
Combined systems	Cäsar with additive Code with additive Double transposition Cäsar with transposition Code with transposition

Encipherment and Disguise of Coordinates: In transmitting place data, areas of attack, commitment and concentration, the Russians in Army and Air Force traffic made use of 5-digit coordinates (Gauss-Krüger) which were specially enciphered and inserted in the message text. Before the war a planchette of celluloid had been devised for this purpose which made it possible to pinpoint areas of 1 square kilometer - if necessary areas of one ninth of a square kilometer by adding a sixth digit (1 - 9) or a letter (a - i). On the maps with the scale 1: 100 000 provided for this purpose a 2-digit number was printed beside cities with a population of 10,000. Since only 100 numbers (00 - 99) were available, these had to be repeated many times in view of the size of the country, nevertheless the general area involved and in most cases the appropriate map sheet was known to the cryptographic clerk. The numerical sequence was terminologic and ran from left to right and from top to bottom over the entire European portion of the Soviet Union.

Scheme of a Map Planchette Scale 1:2



After the outbreak of the war the Russians also had to count on the capture of this means of enciphering coordinates and were therefore obliged to resort to another means of camouflage. As time went on the individual units enciphered these coordinates in the most varied fashion, the 1: 100,000 maps with dinomes printed along side the city names were discarded.

One of the most frequent methods of encipherment now was the symbolic or arithmetic addition of two dinomes, in the latter case omitting the hundreds, to the "ab" and "cd" digit elements of the 5-place coordinates while the last digit "e" usually remained unchanged. Reading on the map resulted after decipherment in the sequence: left (right) than upper (lower) margin, the final unenciphered digit of the coordinates gave the subdivision of the one square kilometer area.

In contrast to the Army and the Air Force the NKVD organs employed 4-place coordinates, i.e. without any subdivision of the 1 square kilometer area. The lack of 1:100 000 maps for the Balkans, Hungary, Croatia, Czechoslovakia, and southern Poland resulted in the exclusive use there of 1: 300 000 maps and the 4-place coordinates could only define an area 3 ,3 x 3 .3 kilometers, The most important differences in the use of

coordinates between Army and Air Force on the one hand and the NKVD on the other are found in the fact that the former disguise the coordinates separately while the NKVD organs enciphered them along with the message texts and also in the fact that Army and Air Force could transmit either disguised coordinates or place names enciphered in the text, whereas, the NKVD formations always gave the place and the coordinates one after the other and enciphered them in the text.

The so-called Verst maps used before the war have not been in use since 1939. The Soviet Command today generally uses only maps in the scale 1: 100 000 and 1: 300 000.

C. Explanation of Terms

German Term	English Term	Explanation
Aufgebrochen alphabetisch	Interruptedly alphabetic	A system in which the initial letters do not follow one another alphabetically, while the digraphs, trigraphs, syllables, and words with the same initial do show an alphabetic sequence.
Belegung	Entry	The position (cell) in a code reserved for a letter, digraph, trigraph, syllable, word, sentence, mark of punctuation, number or concept.
Bigramm	Digraph	A pairing of letters or digits.
Blender	Null	A blind, i.e. meaningless number or group which is inserted in the message text.
Caesar	Caesar	The simplest form of substitution system. The plain elements are usually only letters, 1-digit numbers, and marks of punctuation, and these are expressed by various combinations of digits or letters or by both intermingled.
Chispruch	Encrypted message	
Chitext	Encrypted text	
Code	Code	A substitution system of considerable extent which contains in addition to letters, marks of punctuation — often with variants — digraphs, trigraphs, syllables, words, and numbers, phrases, composite concepts, type designations, cover groups, and calls for special entries.
Deckgruppen	Cover groups	Entries in the code which may signify among other things names of persons, cities, service grades, official positions, troop units, etc.
Entschluesseln	To decrypt	To remove the disguise from encrypted messages with the aid of basic cryptographic materials, in contrast to "entziffern" to cryptanalyse.
Entzifferung	Cryptanalysis	The activity which leads to the removal of the disguise from messages encrypted in any fashion without the use of basic cryptographic materials in order ultimately to be able to read the text. The concept "Ziffer" (digit) in this word is thought of only abstractly.
Ersatzverfahren	Substitution system	A system in which the plain element or the plain concept is expressed in each case by combinations of digits, letters, or both, such combinations being of different possible length.
erweiterte Caesaren	Expanded Caesars	Systems which contain in addition to letters, 1-digit numbers, and marks of punctuation, digraphs, syllables, short words, and sometimes also 2-digit numbers.
Es		Abbreviation for Entzifferung

German Term	English Term	Explanation
Feld	Field	Same as Belegung (entry or cell)
Haeufigkeit	Frequency	(In general) the percentual occurrence of letters, digraphs, trigraphs, words and concepts in a language.
Hinweisgruppe	Switch group	A group showing the manner of reading.
Indikator	Indicator	Like Kenngruppe, usually "aufgeschluesselt" or "gegliedert"
Kengruppe	Indicator group	A group which almost without exception can stand among the first or last ten groups of an encrypted message and which indicates the reencipherment and its starting points. The indicator group may be camouflaged, i.e. may also be sent encrypted.
Kombiniert ueber-schluesselte Verfahren	Reenciphered systems	Systems encrypted two or more times, e.g. transposed code, Caesar with additive, double transposition, code with two additives.
Kontroll-gruppe	Control group	A second Kenngruppe similar to the first.
mehrfach belegte Caesaren	Caesars with variants	Caesars which have two or more possibilities of expressing frequently occurring plain elements (variants).
Monogramm		A single letter or digit.
Position		Like Feld, represents the least unit in the structure of a cryptographic system.
Satzbuecher	Code books	Especially large codes with complete sentences (commercial and economic codes).
Schluessel-mittel		Cryptographic systems and systems of reencipherment
Schluesseln, verschluesseln	To encrypt	To disguise plain text by any desired cryptographic means
Spaltencaesar	Polyalphabetic substitution (columnar Caesar)	A system consiting of several Caesars. The individual alphabets are employed successively in rotation.
Symbolische Addition	Symbolic addition	The addition of two digits without carrying the tens (mod 10).
Tauschverfahren		A limited category of substitution systems. In general this designation is selected for substitution by means of a series or a table.
Terminolog-isch	(terminologic)	A directly or indirectly ascending or descending sequence of numbers.
Trigramme	Trigraphs	Combinations of letters or digits having three elements.

DF-196

German Term	English Term	Explanation
Versatzver-fahren	Transposition systems	Systems in which the plain elements are scrambled by certain regular changes of position, e. g. with the transposition box, double box, diagonal transposition, raster, machine ciphers.
Wuerfel	Transposition system	Transposition systems in which the plain elements are entered in an outlined rectangle from left to right, row by row, and are then taken out column by column according to a key and transmitted as a cipher message after being divided into groups.
Wurm	Additive	Same as Zahlenwurm. An unsystematic, virtually endless sequence of digits which is added symbolically (mod 10) to an encrypted text as reencipherment.

~~TOP SECRET~~

PART III. THE STRUCTURE OF THE RUSSIAN CRYPTANALYTIC SECTION IN THE FORMER GERMAN ARMY AND A CRITICISM OF ITS ORGANIZATION DEFECTS

For the clarification of Russian radio traffic there existed in the former German Army an extensive and widely ramified organization at the head of which stood as directing and commanding unit the Signal Intelligence Agency (General der Nachrichten Aufklaerung, abbreviated Gen d NA). Subordinate to this highest unit in regard to assignment and personnel were from three to five Signal Intelligence Evaluation Centers (Nachrichten Aufklaerungs Auswertestellen, abbreviated NAAS), (the so-called Horch-Kommandeure), and a Signal Intelligence Battalion Finland (Nachrichten Abteilung Finnland). A schematic representation of this organization is as follows:

	Gen d NA						
1941	-	-	1	2	-	3	-
1942	6	-	1	2	-	3	NA
1943	-	8	1	2	6	3	NA
1944	-	8	1	2	6	3	NA
1945	-	8	1	2	-	3	-

Explanation: 1 = NAAS 1 (Nachr. Aufkl. Ausw. St. Süd)
2 = NAAS 2 (Mitte)
3 = NAAS 3 (Nord)
6 = NAAS 6 (Kaukasus, ab 1943 Benden)
8 = NAAS 8 (Südukraine)
NA = Nachr. Abtlg. Finnland

The signal intelligence evaluation centers (NAAS) arose from the fixed intercept stations (Feste Horchstellen) formerly the fixed radio receiving stations (Feste Funk-Empfangsstellen), which were operated in peacetime in Breslau, Treuenbrietsen, and Koenigsberg.

Subordinate to the NAAS, which were normally located in the same place with the Commander-in-Chief of Army Groups, were fixed intercept stations, intercept companies (Horchkompanien), and long-range signal intelligence platoons (Fernaufklaerungszuege). While the fixed intercept stations and long-range signal intelligence platoons show no further sub-division, close-range signal intelligence platoons (Nahaufklaerungszuege) and direction finding

~~TOP SECRET~~

platoons (Feldwege) were employed further forward by the intercept company.

The close-range signal intelligence platoons and direction finding platoons whose task consisted in the interception of enemy messages according to directives from the intercept companies and in the location of unknown radio stations by direction finding, forwarded their results without working them over to the respective intercept companies, which on their part did cryptanalytic work on the simplest systems. The intercept companies sent traffic which they could not solve to the signal intelligence evaluation centers (NAAS).

The fixed intercept stations and the long-range signal intelligence platoons were intercept stations somewhat farther removed from the front which were to work primarily according to directives issued through the NAAS by the Gen d NA. The traffic intercepted was likewise sent to the NAAS.

The task of the NAAS was the decipherment and evaluation of the traffic supplied by their subordinate organizations. For this purpose the NAAS had a considerable number of cryptanalysts at their disposal whose task it was to work on relatively small systems of medium difficulty of the Army and the Air Force and to report the content of these messages through evaluation section to the Intelligence Section of the Army Group as well as to the evaluation center of the Gen d NA. In these cryptanalytic efforts the NAAS were given technical direction by the cryptanalytic section of the Gen D NA and were currently informed regarding advances in the science of cryptanalysis.

The activity of the NA-Finnland corresponded essentially to that of the NAAS; however, this unit was smaller in size and in certain matters coordinated its work with the Russian cryptanalytic section in the Finnish Army.

The NAAS and the NA-Finnland sent carbon copies of all traffic with a notation "worked on" or "not worked on" to the Gen d Na. All 5-digit traffic of the Army and Air Force as well as all NKVD messages were reserved exclusively to the Gen d NA. The forwarding of material which had been worked on to this central office served for a control of the cryptanalytic

DF-196

activity of the NAAS, and gave opportunity for correction and support where necessary.

The results of all deciphered messages were combined by the evaluation section of the Gen d NA into a daily report - "intercept situation" ("Horchlage") and laid before the interested authorities.

Certain defects in the collaboration between the Gen d NA and the NAAS, defects which will be taken up in detail in our criticism, gave occasion for the formation of two fixed intercept stations directly subordinated to the central unit.

The personnel strength of the entire organization can, of course, be given only in approximate average figures because it was subject to constant, and in part considerable variations. Around the turn of the year 1944/45 the German Army signal intelligence effort against Russia was probably constituted somewhat as follows:

	0	1	2	3	4	5	6	7	8	9
Gen.d.NA	30	50	15	30	6	-	-	20	5	50
Fe.H.St.6	-	-	-	-	10	90	10	10	2	10
Fe.H.St.11	-	-	-	-	15	120	20	10	3	12
NAAS 8	15	35	8	10	30	300	40	20	20	80
NAS 1	15	35	8	10	30	320	40	20	20	80
NAAS 2	20	40	10	15	40	350	50	20	20	90
NAAS 3	15	35	8	10	30	300	40	20	20	80
	95	195	49	75	161	1480	200	120	90	402

In all therefore 3867 persons

Explanation: 0 = Cryptanalysts

1 = Cryptanalytic assistants

2 = Content evaluators

3 = Assistants in evaluation

4 = Traffic, operational and D/F evaluators.

5 = Intercept operators.

6 = D/F operators

7 = Teleprinter operators

8 = Technical personnel

9 = Administration

Years of work in a key position in the central agency of this apparatus gave the authors of this report a chance to recognize a number of serious defects, both in the manner in which the work was done and in the structure of the organization.

1. The administration both at the central agency and at the subordinate organizations had little or no technical knowledge in this field. Therefore it was not in a position to guarantee expert guidance for the entire apparatus and for its constituent parts and faced the difficulties, which naturally arose in the separate fields of endeavor, with a complete lack of understanding and often with a lack of interest. Therefore for the most part it proved an obstacle rather than an aid to the work. It was unmistakably the desire of the administration to swell the operational figures artificially for the purpose of increasing their own personal importance through the size of the unit.
2. Since the NAAS were located in the vicinity of the top command of the Army Groups, a close contact necessarily resulted between the intelligence section of the Army Group and the evaluation section of the NAAS which finally had the result that the direction of the NAAS in a technical respect corresponded less to the requirements of the central agency than to the desires of the commander. This could not fail to cause friction between the NAAS and the central agency and this had a very unfortunate effect on the results of the work.
3. The splitting up of the cryptanalytic work between the central agency and the NAAS with their intercept companies had as a result that, along with an enormous "paper war" - one original and two carbons of every radiogram for the central agency, NAAS and the intercept company - there was almost always duplication of effort in decipherment and evaluation. It even happened that one and the same message was intercepted by the intercept companies of several NAAS and was processed almost simultaneously at all these stations. With the set-up of the entire organization as described such duplication of effort was hardly to be avoided.

4. The duplication of effort which has just been criticized was not infrequently the result of a perfectly false ambition on the part of the administration of the individual stations. Knowing that a particular system was already being worked on successfully by another unit, one tried for purely competitive reasons to effect a new solution of the system in order to dispute the right of the original party to credit. In spite of a regular exchange of solved systems between the individual stations this was quite possible without arousing the suspicion of plain copying since the courier connections were often poor.

5. The worst disturbance of the professional work both at the central agency and at all its subordinate stations was caused, without a doubt, by the purely mechanical handling of this apparatus. The treatment of the workers was not according to their professional ability and performance, but exclusively according to their military rank. Military service, such as drills, firing practice or terrain exercises were taken so seriously that the scientific work of the cryptanalyst could not fail to suffer in consequence. By way of comparison it may be stated that relatively far more was accomplished when the organization had a civilian character during peacetime.

This enumeration makes no claim to completion. The authors have merely sketched here the most striking and perhaps the most serious defects. A number of other inadequacies might be criticized but these may have had a less unfavorable effect on the work.

The unmistakable consequence of all these defects was an extremely unproductive waste of energy which resulted in the creation of a decided over organization which ran idle to a great extent. With expert, sensible planning as much or more might have been accomplished with a far smaller apparatus which would have been simpler in structure and easier to supervise.

SUGGESTION FOR FORMATION OF A RUSSIAN CRYPTANALYTIC UNIT

DF-196

SUGGESTION FOR FORMATION OF A RUSSIAN CRYPTANALYTIC UNIT

A state interested in the preservation of its own vital interests and those of its citizens must seek a maximum degree of military security. It can meet this need only if it keeps careful watch on its surroundings in order to draw the necessary inferences from the appearance of any threatening constellation, and thus take defensive measures before all its powers have to be employed in defense. It must not content itself with observation of momentarily hostile or ill-disposed powers, for the experience of the last few years shows clearly that today's friends may be tomorrow's foes. This watch must be all the closer, the greater the gap between the ideologic views of the observer and those of the observed, and the smaller the spatial separation between the two, because then the possibility of a sudden violent break may develop most quickly.

The most watchful and incorruptible eye of a state is a well organized cryptanalytic agency staffed with experienced specialists since, in contrast to most other government bureaus, it draws its information directly from reports which the observed government composes for its own use. Hence it offers purely factual reports, free from any bias, intentional or unintentional. Cryptanalysis is, to be sure, a relatively young science calling for further development, yet its achievements in the field of intelligence are already undeniable.

Adequate ability and tested experience in cryptanalytic and organisational work, together with personal reasons of a politico-philosophic nature, moved the undersigned, even before the expected Allied victory, to propose as early as possible to the appropriate offices of the United States Army the formation of a Russian cryptanalytic unit and to offer to undertake the organization and conduct of such a group.

The undersigned are in a position to name a number of capable, fully trustworthy members of their former units who have given assurance of their willingness to work in the interest of the USA. Although contact with most of these persons has been lost, enough information is at hand regarding their location so that a majority could be assembled.

DF-196

Under reference to the undersigneds' report on the Russian cryptanalysis of the former German Army, especially the parts regarding the organization and criticism of it, the undersigned suggest the formation of a cryptanalytic section for Russian along the following lines:

1. A central cryptanalytic organization to handle all analytic work. This will be set up to include units for the direction of the actual decryptment, control of the intercept stations listed below, administration, records, and archives, the cryptanalytic section proper, evaluation for its own analytic purposes with appropriate card indices, research on radio operations, and liaison with the evaluation organization which must exist at United States Headquarters in Europe. The personnel strength of the central organization would have to be about 86 persons. Of these 46 would be qualified specialists whom the undersigned could, if need be, provide. The remaining 40 persons (who might for the present be women) would need — besides the willingness to work — a certain degree of intelligence and some knowledge of Russian. The undersigned do not doubt that they can assemble the necessary personnel. For liaison with the United States Army agency two or three good interpreters for Russian and German would be necessary, since the working language of the section for decryption would necessarily be Russian.

Adequate space (about 800 - 1000 square meters) to assure quiet, intensive work, preferably in a building apart, would be necessary. In addition to ordinary office equipment including some four typewriters with Latin type and two with Russian type, provision must be made for printing under security regulations the requisite forms to meet current needs.

It would be expedient to have the cryptanalytic unit somewhere near the evaluation center at headquarters.

2. A main intercept station, as near as practicable to the cryptanalytic unit. The purpose of this station is to work traffic of special interest to the cryptanalytic unit, i.e. to increase and also expedite reception of such traffic. This intercept station would need 25-30 receivers and all other

necessary technical equipment. Work must be carried on in four shifts. Personnel strength would be approximately:

1 Station Director
1 Personnel Expert
3 Technical Experts
5 Evaluators
120 Intercept Operators

or all told some 130 persons. It is assumed that the equipment and space requirements of such a station are familiar.

3. Three advance intercept stations; in southern, central and northern areas, charged with current reception of Russian traffic according to instructions from the cryptanalytic unit. These stations carry out range findings and provide traffic analysis. In strength they would correspond closely to that of the main station, but require in addition about 10 direction finding operators each, i.e. some 140 persons in all.

4. A swift, dependable system of communication between the main station and the advance stations, for the transmission of orders from the cryptanalytic bureau and of questions from the out-stations. In addition to telephone connections there should be teleprinters for the cryptanalytic bureau and each of the four stations.

Transmission of intercepted messages from the intercept stations to the cryptanalytic unit would be both by teletype and courier. Sending by teletype would call for two machines at each intercept station and five at the cryptanalytic unit with some 25 persons (chiefly women) to operate them. Courier connection could be by air or rail and might call for 15 persons.

Broken down by specialities, the personnel needs of the entire organization would therefore be as follows:

~~TOP SECRET~~

	a	b	c	d	e	f	g	h	i	j	k	l	
1	2	35	6	40	3	-	-	-	-	-	-	-	86
2	-	-	-	1	3	1	120	-	5	-	-	-	130
3	-	-	-	1	3	1	120	10	5	-	-	-	140
4	-	-	-	1	3	1	120	10	5	-	-	-	140
5	-	-	-	1	3	1	120	10	5	-	-	-	140
6	-	-	-	-	-	-	-	-	-	25	-	-	25
7	-	-	-	-	-	-	-	-	-	-	4	15	19
	2	35	6	44	15	4	480	30	20	25	4	15	= 680

Legend

a. Director of Organization
b. Cryptanalysts
c. Research man on Radio Operation
d. Assistants
e. Technicians
f. Station Director
g. Intercept Operators
h. Direction Finding Operators
i. Evaluators
j. Teleprinter operators
k. Page Printers
l. Couriers

1. Central Unit
2. Main Intercept Station
3. Southern Intercept Station
4. Central Intercept Station
5. Northern Intercept Station
6. Transmission Net (administrative)
7. Transmission Net (operational)

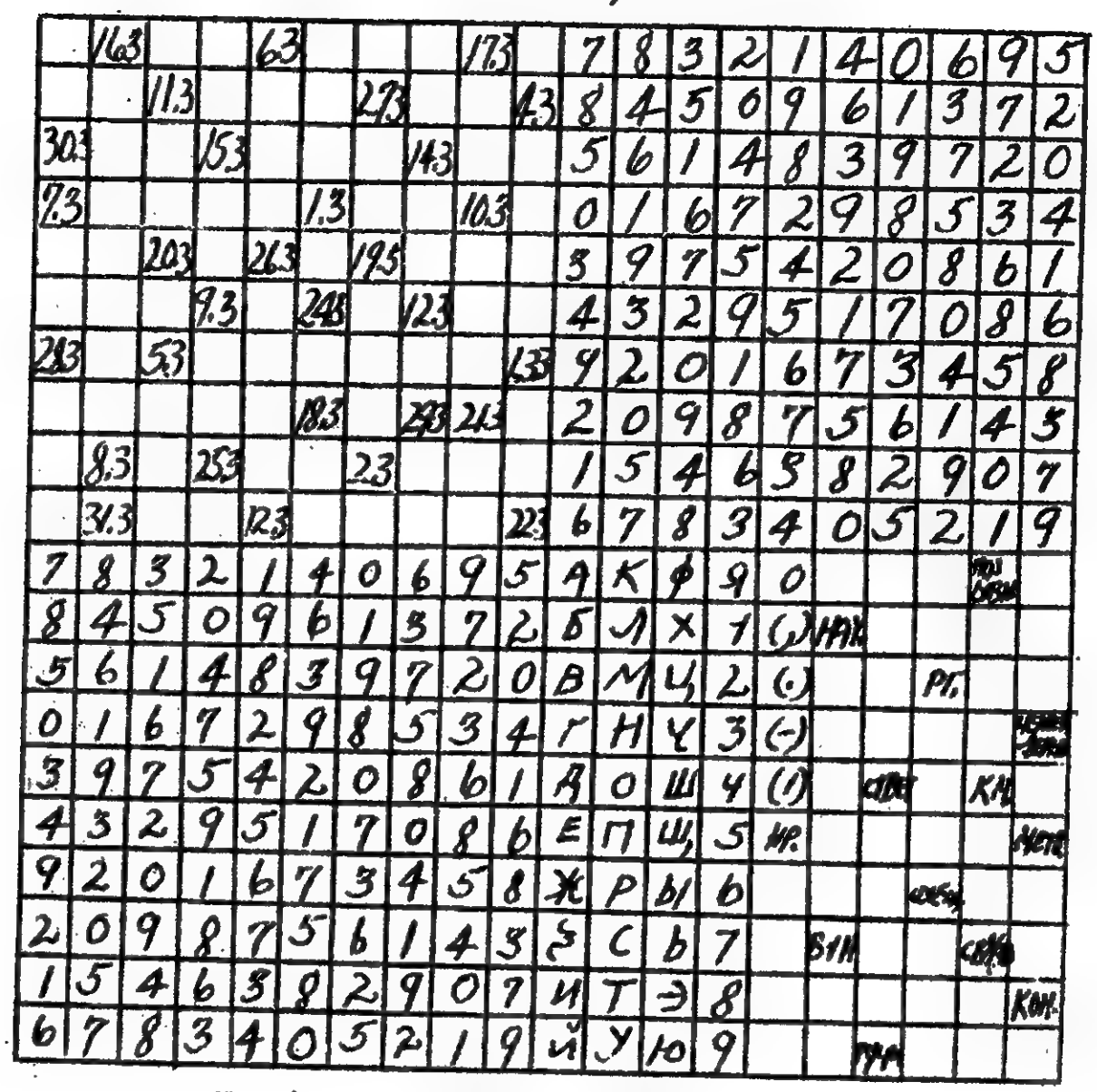
For the sake of expediency it is necessary to give the cryptanalytic unit a completely civilian appearance, subordinated, of course, to the direction and guidance of the United States Army. Intercept stations need not be staffed with civilians; they might be operated by US Army personnel. Men from the former German Army could be employed, if needed. The same is true for the transmission service and couriers.

The proposed organization would represent about one-fourth the personnel employed for the task by the former German Army. The undersigned know, however, from experience that even with such a limited organization, but with uncompromising leadership, a maximum of decryption and evaluation could be done. Hence they would be in a position to obligate themselves to produce satisfactory results within a short time with the organization proposed or with one similar to it.

/signed/ DETTMANN

SAMSONOW

Plate I: "ПТ-35" with data for March



Russian 2-Digit Substitution

Plaintext: ВАШ ПОЗЫВНОЙ -4Т1-

Translation: Your call sign is 4t1.

Cipher text (Key of 19.3.): 93,03,47,06,84,45,29,19,84

Plate 2 : "ЛТ 39"

	2	3	9	8	0	6	4	1	7	5
6	А	К	Ф	Я	σ	ПОЛК			СРОУМ	
3	Б	Л	Х	1	(,) МИЛУТ					
4	В	М	Ц	2	(·)	ПЕРЕ ДАТМ		СВЯЗЬ		
7	Г ЛОНАР	Н	Ч	3 КМ	(-)		ЛАБОТ		СТАНЦ	
0	Д	О	Ш ДАНН	4	(/)		ГАЛП	СЕТЬ	ЧС	
9	Е	П	Щ	5	ИР.		РГ.			ЧАС
1	Ж	Р	Ы ДИВ	6			РЯМ			
8	З БАГ.	С	Ь	7		НИК		СОБОТ		
5	И	Т	Э	8	ОТВЕТ		Ч.Б.		ТЕЛЕ ГРАФ	
2	Й	У	Ю	9 МЕТР.						ШТАБ

Russian 2-digit Cäsar-
(double readings)

Plaintext: СООБЩИТЕ ДАННЫЕ НА 15.9.

Translation: Give the (radio) data for 15.9.

Cipher text: 07,81,09,54,73,62,38,98,40,28,40-

Plate 3 : "ПТ 41"

	4	1	9	8	0	7	3	2	6	5
6	В	/	И [illegible]	О	Н КТО	Ч РОТА	К	Z	А МЫ	Ч АНВ
3	Р ВАМ	Ь	Б	Т РАЛНО	Ы	П РТ	Z	Ж ПОМ	Ф	Е
2	Й	Ж ВЪВОД	Ф	Ч.Б	О	В	С ТЕЛЕ ГРАФ	(·)	Ы	О
8	7	Ч	(-) ЗАМ	Л	Ю	И СТАНЦИ	Ц	Г НЕТ	Н КОМ	4
5	Л [illegible]	«	А	Щ ВАС	/	Н БАТ	8 ПРИЕМ НИК	У	7	К НАШ
0	(,)	П ГАЕ	(?)	Х	Ц [illegible]	(·)	Е	С ПОЛК	Р	Ш
7	Е РАБОТ	4	Щ	С	8 НЕМЕЯ ЛЕЛИ	Ъ	Ь РАУН	Я	А ЦАМ	9
1	У	О [illegible]	В	»	Т КЛАА	5	З СРОЧНО	М	ЧС	Т
9	Ю	Г	(-) КОТАА	9	Ш	М ВОЛН	5	О ВЫ	(·)	5
4	З [illegible]	Н	Б	Д ВАШ	Ь	Х	Р	Ч ПЕРЕ-ЛАТЧИК	И	Ъ

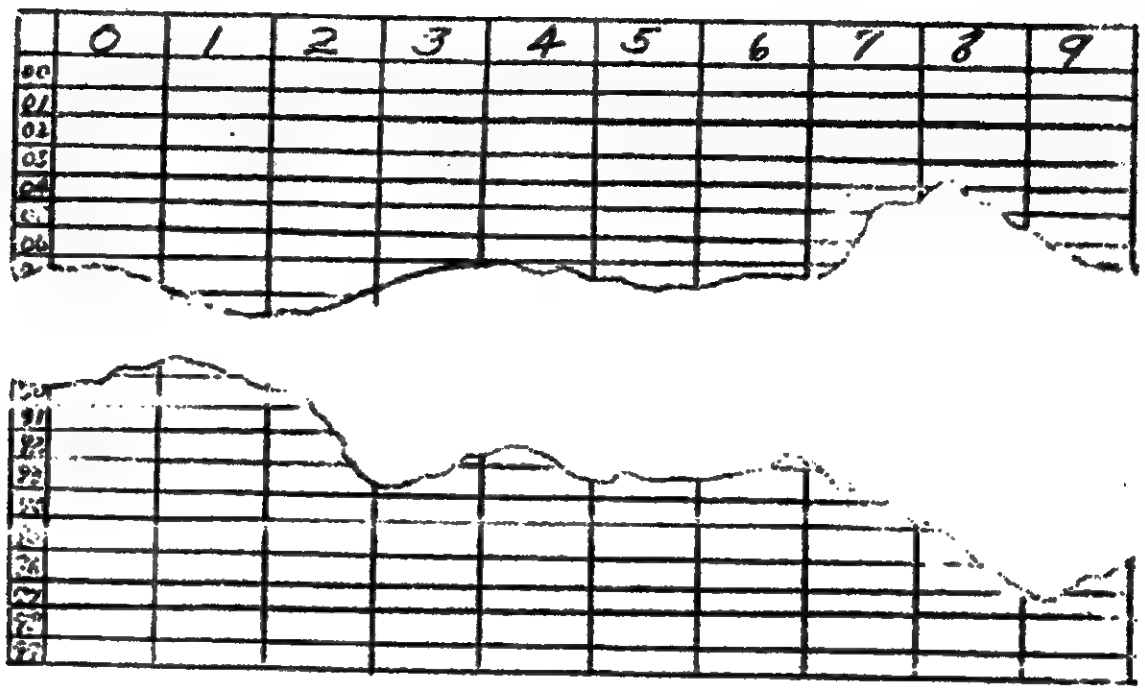
- Russian 2-digit Cäsar with variants -
(double readings)

Plaintext : НАШ ПРИЕМНИК ОТКАЗАЛ, ДАЙТЕ ПО ТЕЛЕГРАФУ.

Translation : Our receiver has gone bad, send by telegraph.

Cipher text : 16, 55, 53, 28, 20, 10, 55, 66, 45, 59, 88, 04, 48, 76, 42, 38, 35, 01, 92, 16, 23, 28, 22 —

Plate 4: (Schematic representation of the first general airforce code).



Entries in Column "0"

А	КО	У	ГРАДУС	0
Б	ЛИ	Ф	МИНУТ	10
В	МА	Х	ГАС	20
ВАМ	НА	Ц	МЕТР	30
ВАС	НЕ	Ч	КМ	40
ВАШ	НИ	Ш	ПЛЮС	50
ВАЛ	НО	Щ	МИНУС	60
Г	О	Ъ	БАЛ	70
ГО	ОБ	Ы		80
Д	ОТ	Ь		90
ДА	П	Э	С	100
Е	ПЕР-	Ю	СО	500
ЖЕ	ПО	Я	СОО	1000
ЗА	ПРЕД	(.)	1	1500
И	ПРИ	(-)	2	2000
К	РО	(/)	3	2500
Л	С	(:)	4	3000
М	СА	(,)	5	3500
К	Т	НОМЕР	6	4000
			7	

Entries of columns 1 to 7: alphabetical vocabulary.

Plate 5: Schematic Representation of One Page of "RAK 39"

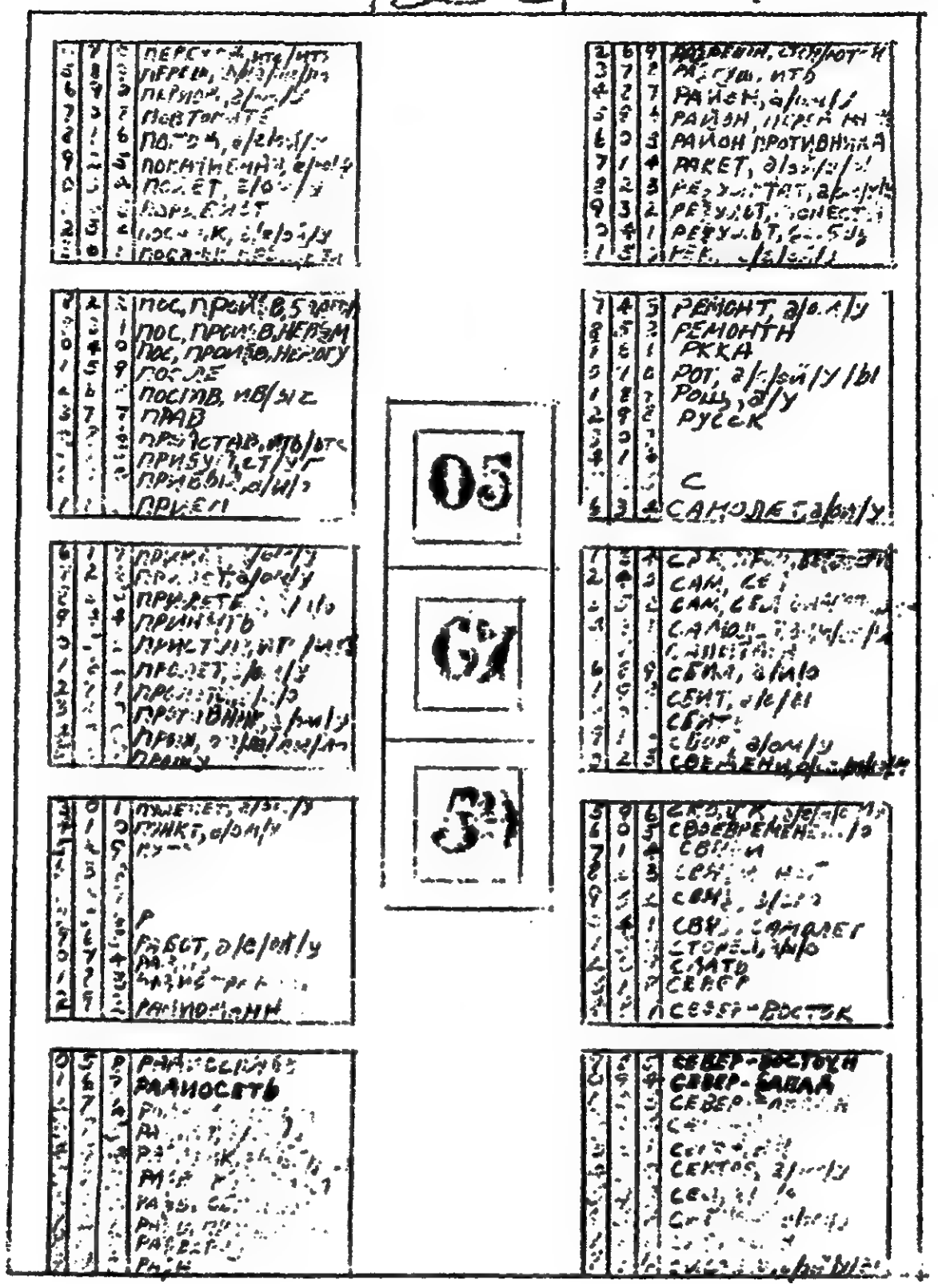
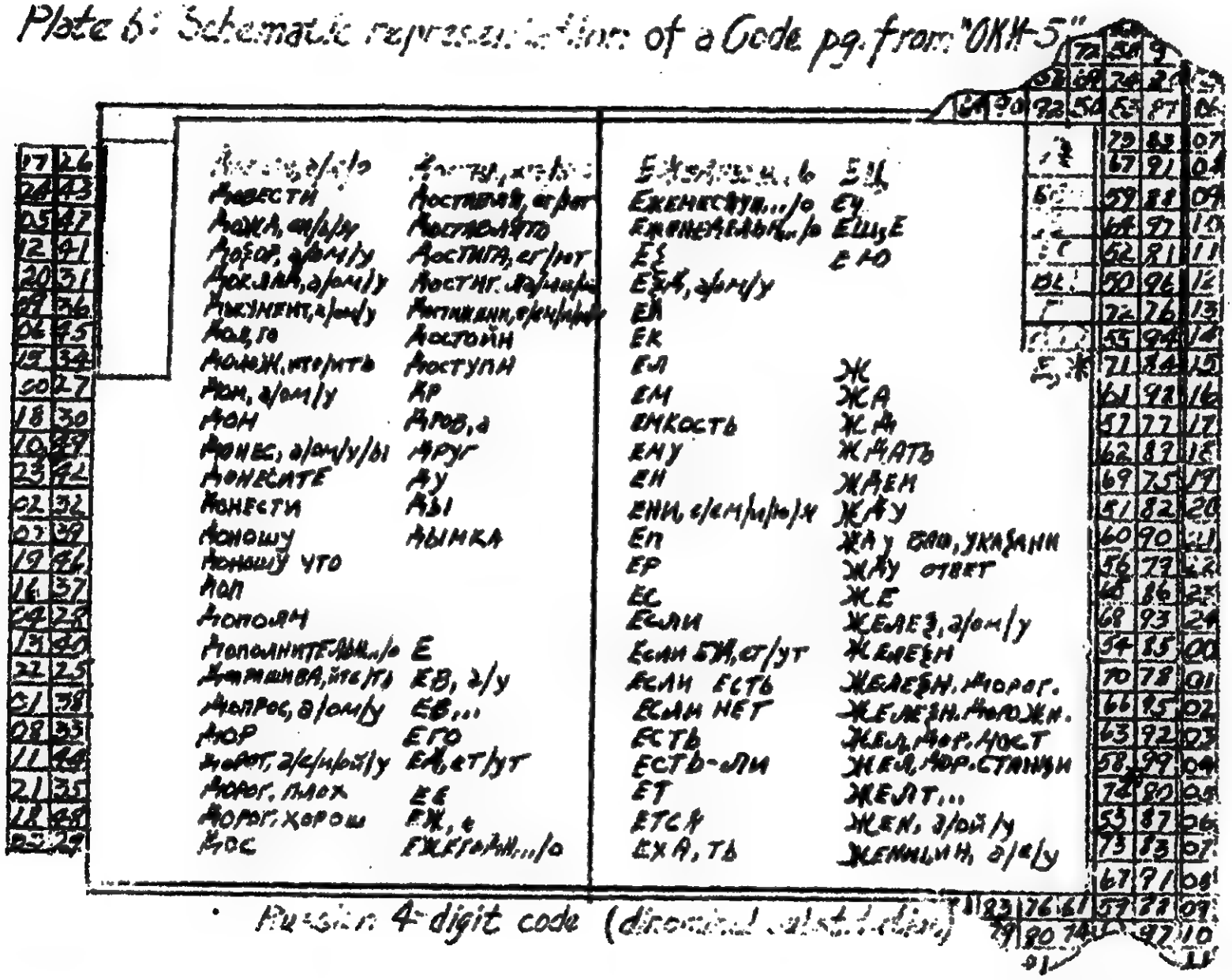


Plate 6: Schematic representation of a Code pg. from "ОКН-5"



Russian 4-digit code (decimal substitution)

TOP SECRET

Plate 7: Cäsar
"Border Guard North" (Leningrad and Kasastan)

	Д	К	Ф	Е	С	Р	Ч	Л	Ь	Щ
8	О		А	Б	У	Ф	Х			
3		И	В	Г	Ц	Ч	Ш			
9			2	Д	Щ	Ы	Ь			
1			Е	З	Э	Ю	Я			
6			Ж	З	4	Й				
4			И	К		5				
5			Л	М		(.)	6			
0			Н	О		(-)		7		
			П	Р		НР			8	
			С	Т		(,)				9

Russian 2-digit-letter substitution

Plain text: КОМ.БАТ.ПРИБЫЛ ПРИВЕТ БОГОМОЛОВУ

Translation: The battalion chief has arrived.
greetings to Bogomolov

Cipher text: 4E,0E,5E,5Р,9E,4Ф,3Ф,5Р,7Ф,7E,4Ф,8E,9Р,
7Ф,7Ф,7E,4Ф,3Ф,1Ф,2E,8E,0E,3E,0E,5E,0E,5Ф,0E,3Ф,8C,5Р—

Plate 8: Cäsar
"Coast Guard Odessa"

	8	3	1	4	7	2	5	0	9	6
3	SAH	KOM	Нет	ПОМ						
7		гул			ИЖК					
0	А	Б	В	Г	Д	Е	Ж	З	О	!
9	И	Й	К	Л	М	Н	О	П	2	3
8	Р	С	Т	У	Ф	Х	Ц	Ч	4	5
1	Ш	Щ	Ы	Ь	Э	Ю	Я		6	7
4	(.)	( )	(-)	НР.					8	9
6			ВО.Н		ЦИСТ				КМ	
2	МАР	НАЧАЛОТВЕТ	ПЕРЕД			ПОДПИ			ПЕРЕД	РТ.
5	РАЗ				СЕГО			ЧТК.		

Russian 2-digit Cäsar with nulls

Plain text: НАЧТ = ОТВЕТ НА НАШ ... ПР 726

Translation: Answer our radio ... 785

Cipher text without nulls and divided into group

07,06,93,21,02,21,92,08,92,08,18,63,26,44,16,19,95,43

Cipher text in the message: 07:06 93621 12:21

92408 72:08 18584 26744 16877 56:43

Plate 9: Cäsar

"Border Guard Transcaucasia"

	4	1	9	6	3	0	8	5	2	7
8	О		А	ВАШ	Б	ВАС	В	ГО	Г	ГУШ
5	ГДЕ	І		Д	ДО	Е	КО	Ж	ЗА	З
6	И	ИЗ	2	И.З	Й	ПА	К	КОМ	Л	БРИ
1		М	ПЛЫ	3	НЕ	Н	ВАУ.	О	ОТ	П
4	Р	ПО	С		Т	НИКЕ	Т	НЭ	У	КОМ
0	ГГ	Ф		Х		5		Ц		Ч
9	ЩИ		Ы		Ь	ПОСТ	Б		Ь	
2		Э		Ю		Я		Ч		ПА
7	(.)		(.)		(-)		ПЯТЬ		Ъ	
3		УМ		УК		ПОЕЗД				З

Russian( ) 2-digit Cäsar

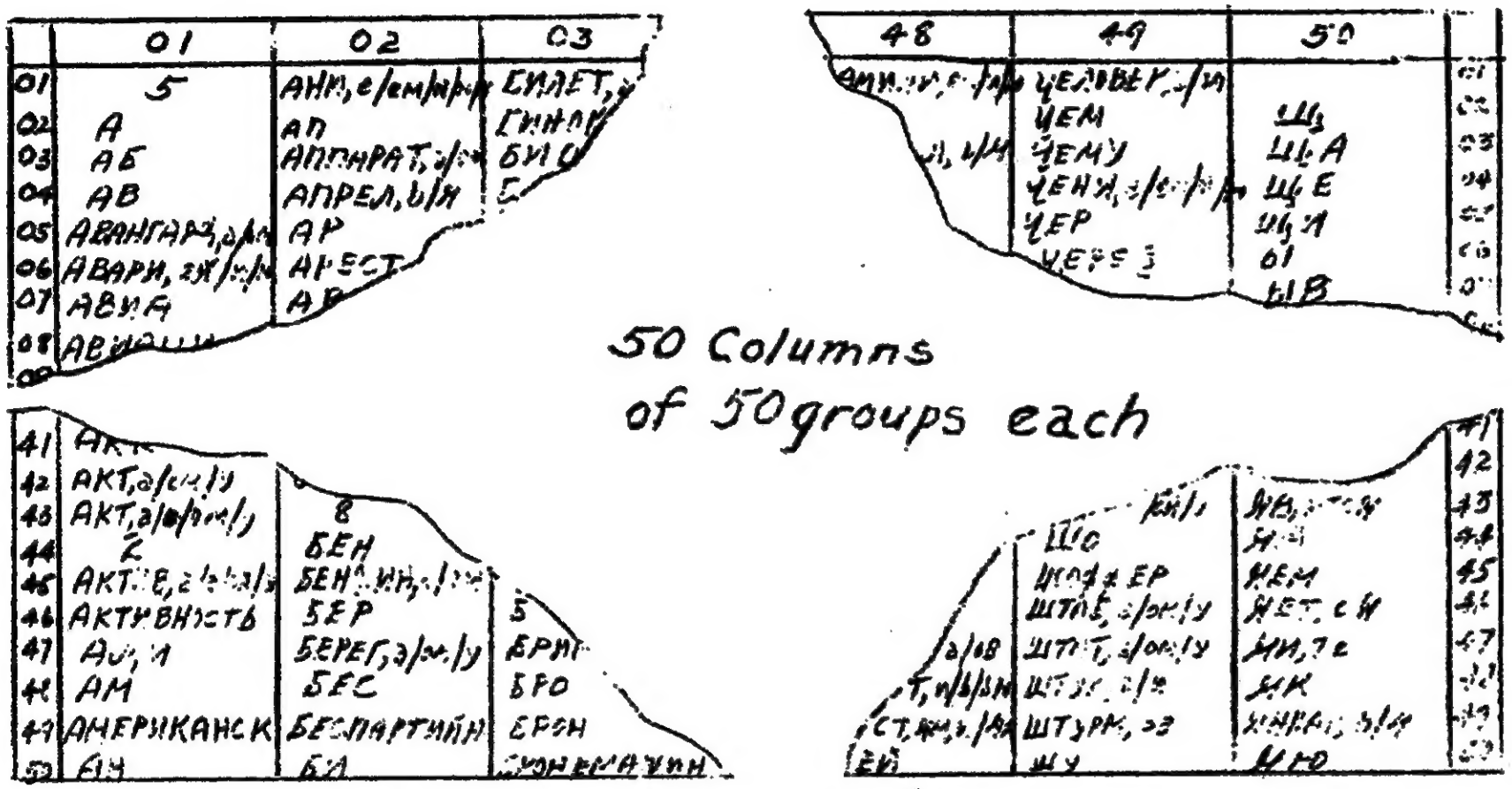
Plain text: ВАШ ПОСТ ГДЕ НАХОДИТСЯ ВАШ ПК (паровой кат

Translation: To the Post Commander, Where is our PK (steam cutter)?

Intermediate text: 16 11 15 49 42 | 89 79 54 10 89 | 06 15 56 64 42 | 49 30 10 89 74 | 17 19 68 79 —

Cipher text: 18041 89691 — 17121 79509 — 15516 54602 — 91691 90499 — 43460 99590 —

Plate 10: Scheme of Code Table "ЭЛЕКТРОН"



Russian 4-digit code (dinome substitution)

TOP SECRET

TOP SECRET

SUMMARY of the most IMPORTANT SYSTEMS of the RUSSIAN ARMY, AIR FORCE and NKVD USED and DECIPHERED during the WAR.

DF-196

SYSTEM	ORIGINAL DESIGNATION	SIZE IN GROUPS	PERIOD OF USE (Month, YEAR) FROM	TO	SERVICE: ARMY	AIR	NKVD	TYPE: "CHIFFRE"	CODE	CODE TABLE	"SUV"	"PT"	REENCIPHERMENT: DOUBLE ADDITIVE (GAMMA)	ADDITIVE (GAMMA)	ADDITIVE (BOOK)	ADDITIVE (ROW)	DINOME SUBSTITUTION	MONOME SUBSTITUTION	MIXED SUBSTITUTION	ADDITION	TRANSPOSITION	REMARKS
5-PLACE CHIFFRE CODE	"091-A"	23 000	III 44	V 45	X	X		X														
"	"062-A"	22 000	III 43	III 44	X	X		X														
"	"045-A"	21 000	III 42	III 43	X	X		X														
"	"023-A"	20 000	X 41	III 42	X	X		X														
"	"011-A"	19 000	I 41	V 41	X	X		X														
4-PLACE NON-ALPHABETIC CODE	—	10 000	X 44	V 45			X		X				X	X								With VARIANTS, SINGLE, LATER DOUBLE ADDITIVE
"	—	10 000	V 43	V 45			X		X				X			X						ROW ADDITIVE, LATER DOUBLE ADDITIVE
"	—	10 000	I 42	I 45			X		X					X								
"	—	10 000	I 42	V 43			X		X						X						X	TRANSPOSITION, LATER BOOK ADDITIVE
4-PLACE ALPHABETIC CODE	—	10 000	X 40	I 42			X		X						X		X					MONOME SUBSTITUTION, LATER BOOK ADD.
"	"ОЦКК-7"	10 000	VII 41	III 42	X				X							X						
"	"ОККФ"	5 000	I 42	III 42	X	X			X							X						
"	"ОКК-7"	5 000	IX 41	I 42	X	X			X							X						
"	"ОКК-6"	5 000	VI 40	III 41	X	X			X							X						
"	"ОКК-5"	5 000	VI 39	VI 40	X	X			X							X						
"	—	3500	VIII 38	I 43			X		X								X					NKVD RESERVE CODE
5-PLACE ALPHABETIC CODE TABLE	—	2500		V 45			X			X								X				COMBINED DINOME-MONOME SUBSTITUTION
4-PLACE ALPHABETIC CODE TABLE	"ЗЕРНО"	2500		V 45			X			X						X						
"	"НИВА"	2100	II 45	V 45			X			X						X						
"	"ВИЗА"	2000		V 45			X			X						X						VARIOUS REENCIPHERMENTS
VARIOUS 3-, 4-PLACE SYSTEMS	"СУВ"	up to 2000	III 42	V 45	X	X					X											ALL TYPES checked HAVE BEEN USED.
VARIOUS 2-, 3-, 4-PLACE SYSTEMS	"ПТ"	up to 500		33 V 45	X	X						X										

PLATE II.

TOP SECRET